(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－100116
（P2002－100116A）
(43)公開日　平成14年４月５日(2002.4.5)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｇ１０Ｌ　11/00		Ｇ１０Ｌ　9/00	Ｅ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	
			６７３Ｅ	
			６７３Ｄ	

審査請求　未請求　請求項の数149　ＯＬ　（全 25 頁）

(21)出願番号　特願2000－260467(P2000－260467)

(22)出願日　平成12年８月30日(2000.8.30)

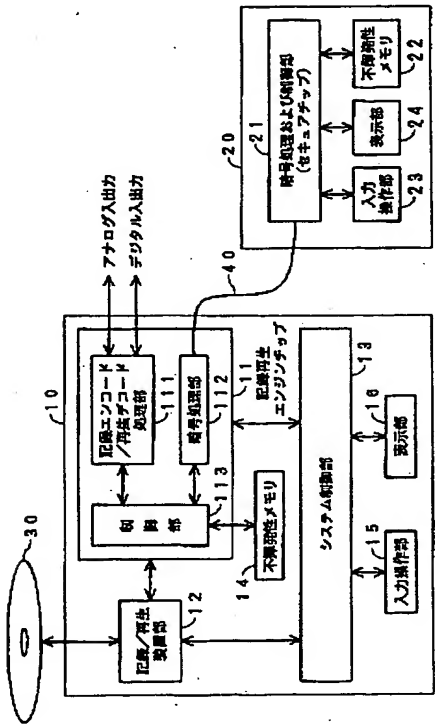
(31)優先権主張番号　特願2000－216388(P2000－216388)
(32)優先日　平成12年７月17日(2000.7.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　猪口　達也
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100091546
弁理士　佐藤　正美

最終頁に続く

(54)【発明の名称】　データ記録再生方法および装置、データ記録装置および方法、データ再生装置および方法並びに記録媒体

(57)【要約】
【課題】　個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止する。
【解決手段】　所定の記録データの記録時には、ユーザＩＤモジュール２０を記録再生装置１０に接続し、使用者を特定するための使用者識別情報をユーザＩＤモジュールから取得して、記録データと共に、記録媒体３０に記録する。所定の記録データの再生時には、記録媒体３０からの情報から検出された使用者識別情報と、不揮発性メモリ１４から読み出した使用者識別情報とが一致したときは、記録情報の再生を許可する。



1

【特許請求の範囲】

【請求項１】記録データの記録時には、使用者を特定するための使用者識別情報を、前記記録データと共に、記録媒体に記録し、

前記記録データの再生時には、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときは、前記記録データの再生を許可することを特徴とするデータ記録再生方法。

【請求項２】請求項１に記載のデータ記録再生方法において、

前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記再生時には前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生方法。

【請求項３】請求項１に記載のデータ記録再生方法において、

前記記録データは、暗号化されており、前記再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生方法。

【請求項４】請求項３に記載のデータ記録再生方法において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生方法。

【請求項５】請求項１に記載のデータ記録再生方法において、

前記記録データの記録時には、記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得するようにすることを特徴とするデータ記録再生方法。

【請求項６】請求項５に記載のデータ記録再生方法において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生方法。

【請求項７】請求項５に記載のデータ記録再生方法において、

前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生方法。

【請求項８】請求項５に記載のデータ記録再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録再生方法。

【請求項９】請求項５に記載のデータ記録再生方法において、

2

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生方法。

【請求項１０】請求項１に記載のデータ記録再生方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生方法。

【請求項１１】請求項１に記載のデータ記録再生方法において、

前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生方法。

【請求項１２】使用者を特定するための使用者識別情報を取得するための第１の使用者識別情報取得工程と、

前記第１の使用者識別情報取得工程で取得した前記使用者識別情報を、記録データと共に、記録媒体に記録する記録処理工程と、

前記使用者識別情報を取得するための第２の使用者識別情報取得工程と、

前記記録媒体からの情報から前記使用者識別情報を検出する使用者識別情報検出工程と、

前記使用者識別情報検出工程で検出された前記使用者識別情報と、前記第２の使用者識別情報取得工程で取得した使用者識別情報とが一致するか否かを判定する判定工程と、

前記判定工程において、前記使用者識別情報が一致したと判定されたときに、前記記録媒体に記録されている前記記録データの再生を許可して再生を実行するようにする再生処理工程と、

を備えるデータ記録再生方法。

【請求項１３】請求項１２に記載のデータ記録再生方法において、

前記第１の使用者識別情報取得工程と、前記第２の使用者識別情報取得工程とでは、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用者識別情報を読み出すことを特徴とするデータ記録再生方法。

【請求項１４】請求項１２に記載のデータ記録再生方法において、

前記第１の使用者識別情報取得工程と、前記第２の使用者識別情報取得工程とでは、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得することを特徴とするデータ記録再生方法。

【請求項１５】請求項１２に記載のデータ記録再生方法において、

前記第１の使用者識別情報取得工程では、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得し、

前記第２の使用者識別情報取得工程では、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用

者識別情報を読み出すことを特徴とするデータ記録再生方法。

【請求項１６】請求項１２に記載のデータ記録再生方法において、

前記記録データは、暗号化されており、前記再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記第２の使用者識別情報取得工程で取得された前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生方法。

【請求項１７】請求項１２に記載のデータ記録再生方法において、

前記記録データの暗号化は、前記第１の使用者識別情報取得工程で取得された前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生方法。

【請求項１８】請求項１２に記載のデータ記録再生方法において、

前記第１の使用者識別情報取得工程で、前記使用者識別情報が取得できないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生方法。

【請求項１９】請求項１４または請求項１５に記載のデータ記録再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生方法。

【請求項２０】請求項１４または請求項１５に記載のデータ記録再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生方法。

【請求項２１】請求項１２に記載のデータ記録再生方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生方法。

【請求項２２】請求項１２に記載のデータ記録再生方法において、

前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生方法。

【請求項２３】記録データと共に、使用者を特定するための使用者識別情報を、記録媒体に記録する記録手段と、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記記録情報の再生を許可する制御手段と、

を備えることを特徴とするデータ記録再生装置。

【請求項２４】請求項２３に記載のデータ記録再生装置において、

前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生装置。

【請求項２５】請求項２３に記載のデータ記録再生装置において、

前記記録処理手段は、前記記録データを暗号化して記録する手段を備え、

再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化が解除されることを特徴とするデータ記録再生装置。

【請求項２６】請求項２５に記載のデータ記録再生装置において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ記録再生装置。

【請求項２７】請求項２３に記載のデータ記録再生装置において、

前記記録データの記録時には、記録再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得するようにすることを特徴とするデータ記録再生装置。

【請求項２８】請求項２７に記載のデータ記録再生装置において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生装置。

【請求項２９】請求項２７に記載のデータ記録再生装置において、

前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ記録再生装置。

【請求項３０】請求項２７に記載のデータ記録再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生装置。

【請求項３１】請求項２７に記載のデータ記録再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生装置。

【請求項３２】請求項２３に記載のデータ記録再生装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生装置。

【請求項３３】請求項２３に記載のデータ記録再生装置において、
前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生装置。
【請求項３４】使用者を特定するための使用者識別情報を取得するための第１の使用者識別情報取得手段と、
前記第１の使用者識別情報取得手段で取得した前記使用者識別情報を、記録データと共に、記録媒体に記録する記録処理手段と、
前記使用者識別情報を取得するための第２の使用者識別情報取得手段と、
前記記録媒体からの情報から検出した前記使用者識別情報と、前記第２の使用者識別情報取得手段から取得した使用者識別情報とが一致したときには、前記記録媒体に記録されている前記記録データの再生を許可して再生を実行するようにする再生処理手段と、
を備えるデータ記録再生装置。
【請求項３５】請求項３４に記載のデータ記録再生装置において、
前記使用者識別情報が予め記憶された不揮発性メモリを備え、
前記第１の使用者識別情報取得手段と、前記第２の使用者識別情報取得手段とでは、前記不揮発性メモリから、前記使用者識別情報を読み出して取得することを特徴とするデータ記録再生装置。
【請求項３６】請求項３４に記載のデータ記録再生装置において、
前記第１の使用者識別情報取得手段と、前記第２の使用者識別情報取得手段とでは、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得することを特徴とするデータ記録再生装置。
【請求項３７】請求項３４に記載のデータ記録再生装置において、
前記第１の使用者識別情報取得手段は、記録ないし再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を取得し、
前記第２の使用者識別情報取得手段は、前記使用者識別情報が予め記憶された不揮発性メモリから、前記使用者識別情報を読み出して取得することを特徴とするデータ記録再生装置。
【請求項３８】請求項３４に記載のデータ記録再生装置において、
前記記録処理手段は、前記記録データを暗号化して記録する手段を備え、
前記再生処理手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記第２の使用者識別情報取得手段により取得した前記使用者識別情報とが一致したときに、前記暗号化を解除する手段を備えることを特徴とするデータ記録再生装置。

【請求項３９】請求項３４に記載のデータ記録再生装置において、
前記記録データの暗号化は、前記第１の使用者識別情報取得手段で取得された前記使用者識別情報に関連付けられたものであることを特徴とするデータ記録再生装置。
【請求項４０】請求項３４に記載のデータ記録再生装置において、
前記第１の使用者識別情報取得手段で、前記使用者識別情報が取得できないときには、前記記録データの記録を不可とすることを特徴とするデータ記録再生装置。
【請求項４１】請求項３６または請求項３７に記載のデータ記録再生装置において、
前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されていることを特徴とするデータ記録再生装置。
【請求項４２】請求項３６または請求項３７に記載のデータ記録再生装置において、
前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録再生装置。
【請求項４３】請求項３４に記載のデータ記録再生装置において、
前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録再生装置。
【請求項４４】請求項３４に記載のデータ記録再生装置において、
前記記録データと共に前記記録媒体に記録する前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録再生装置。
【請求項４５】記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致したときに前記記録対象データの記録を許可し、
前記記録対象データと共に、前記使用者識別情報を、記録媒体に記録することを特徴とするデータ記録方法。
【請求項４６】請求項４５に記載のデータ記録方法において、
前記記録対象データおよび前記記録対象データに付随する使用者識別情報は、記録媒体から読み出されたものであることを特徴とするデータ記録方法。
【請求項４７】請求項４５に記載のデータ記録方法において、
前記記録対象データに付随する使用者識別情報は、前記記録対象データから抽出されるものであることを特徴とするデータ記録方法。
【請求項４８】請求項４５に記載のデータ記録方法において、
前記記録対象データに付随する使用者識別情報は、前記記録対象データと共に伝送路を通じて伝送されてくるこ

とを特徴とするデータ記録方法。

【請求項４９】請求項４５に記載のデータ記録方法において、

前記予め用意された使用者識別情報は、不揮発性メモリに記憶されていることを特徴とするデータ記録方法。

【請求項５０】請求項４５に記載のデータ記録方法において、

前記予め用意された使用者識別情報は、記録装置とは別体の使用者識別情報提供装置から取得することを特徴とするデータ記録方法。

【請求項５１】請求項５０に記載のデータ記録方法において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録対象データの記録を不可とすることを特徴とするデータ記録方法。

【請求項５２】請求項５０に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録方法。

【請求項５３】請求項５０に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録方法。

【請求項５４】請求項４５に記載のデータ記録方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録方法。

【請求項５５】請求項４５に記載のデータ記録方法において、

前記使用者識別情報は、前記記録対象データに埋め込んで前記記録媒体に記録することを特徴とするデータ記録方法。

【請求項５６】記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致したときに前記記録対象データの記録を許可する制御手段と、

前記制御手段により記録が許可されたときに、前記記録対象データと共に、前記使用者識別情報を、記録媒体に記録することを特徴とするデータ記録装置。

【請求項５７】請求項５６に記載のデータ記録装置において、

前記記録対象データおよび前記記録対象データに付随する使用者識別情報は、記録媒体から読み出されたものであって、前記使用者識別情報を検出する手段を備えることを特徴とするデータ記録装置。

【請求項５８】請求項５６に記載のデータ記録装置において、

前記記録対象データに付随する使用者識別情報を、前記記録対象データから抽出する手段を備えることを特徴とするデータ記録装置。

【請求項５９】請求項５６に記載のデータ記録装置において、

前記記録対象データに付随する使用者識別情報は、前記記録対象データと共に伝送路を通じて伝送されてくるものであって、前記伝送されてくる信号中から前記使用者識別情報を検出する手段を備えることを特徴とするデータ記録装置。

【請求項６０】請求項５６に記載のデータ記録装置において、

前記予め用意された使用者識別情報は、不揮発性メモリに記憶されていることを特徴とするデータ記録装置。

【請求項６１】請求項５６に記載のデータ記録装置において、

前記予め用意された使用者識別情報は、記録装置とは別体の使用者識別情報提供装置から取得することを特徴とするデータ記録装置。

【請求項６２】請求項６１に記載のデータ記録装置において、

前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録対象データの記録を不可とすることを特徴とするデータ記録装置。

【請求項６３】請求項６１に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化されており、前記暗号化を解除する手段を備えることを特徴とするデータ記録装置。

【請求項６４】請求項６１に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録装置。

【請求項６５】請求項５６に記載のデータ記録装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録装置。

【請求項６６】請求項５６に記載のデータ記録装置において、

前記使用者識別情報は、前記記録対象データに埋め込んで前記記録媒体に記録することを特徴とするデータ記録装置。

【請求項６７】使用者を特定するための使用者識別情報を取得し、取得した前記使用者識別情報を、記録データと共に、記録媒体に記録することを特徴とするデータ記録方法。

【請求項６８】請求項６７に記載のデータ記録方法において、

前記記録データは、前記使用者識別情報に関連付けられた暗号化が施されることを特徴とするデータ記録方法。

【請求項６９】請求項６７に記載のデータ記録方法において、

記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記記録装置に供給するようにし、前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とするデータ記録方法。

【請求項７０】請求項６９に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ記録方法。

【請求項７１】請求項６９に記載のデータ記録方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録方法。

【請求項７２】請求項６７に記載のデータ記録方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録方法。

【請求項７３】請求項６７に記載のデータ記録方法において、

前記使用者識別情報は、前記記録データに埋め込むことを特徴とするデータ記録方法。

【請求項７４】使用者を特定するための使用者識別情報を取得するための使用者識別情報取得手段と、

前記使用者識別情報取得手段で取得した前記使用者識別情報を、所定の記録データと共に、記録媒体に記録する記録処理手段と、

を備えるデータ記録装置。

【請求項７５】請求項７４に記載のデータ記録装置において、

前記記録処理手段は、前記記録データを、前記使用者識別情報に関連付けた暗号化処理して記録する手段を備えることを特徴とするデータ記録装置。

【請求項７６】請求項７４に記載のデータ記録装置において、

前記使用者識別情報取得手段は、別体の使用者識別情報提供装置からの前記使用者識別情報を取得する手段からなり、

前記使用者識別情報提供装置が接続されていないときには、前記記録処理手段による記録処理動作を不可とする制御手段を設けたことを特徴とするデータ記録装置。

【請求項７７】請求項７６に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は暗号化されており、前記使用者識別情報取得手段は、前記使用者識別情報の暗号化を解除する手段を備えることを特徴とするデータ記録装置。

【請求項７８】請求項７６に記載のデータ記録装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ記録装置。

【請求項７９】請求項７４に記載のデータ記録装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ記録装置。

【請求項８０】請求項７４に記載のデータ記録装置において、

前記使用者識別情報は、前記記録データに埋め込まれることを特徴とするデータ記録装置。

【請求項８１】使用者を特定するための使用者識別情報が、記録データと共に記録された記録媒体からの前記記録データの再生方法であって、

前記記録媒体からの情報から前記使用者識別情報を検出し、

前記検出した前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しているかどうかを判定し、

一致しているときには、前記記録データの再生を許可することを特徴とするデータ再生方法。

【請求項８２】請求項８１に記載のデータ再生方法において、

前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記再生時には前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ再生方法。

【請求項８３】請求項８１に記載のデータ再生方法において、

再生装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記再生装置に供給して、前記不揮発性メモリに記憶するようにすることを特徴とするデータ再生方法。

【請求項８４】請求項８３に記載のデータ再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、暗号化して、前記記録装置に供給するようにすることを特徴とするデータ再生方法。

【請求項８５】請求項８３に記載のデータ再生方法において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該使用者識別情報提供装置ごとに固有の情報であることを

特徴とするデータ再生方法。

【請求項８６】請求項８１に記載のデータ再生方法において、

前記記録データは、暗号化されており、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化を解除することを特徴とするデータ再生方法。

【請求項８７】請求項８６に記載のデータ再生方法において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ再生方法。

【請求項８８】請求項８１に記載のデータ再生方法において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ再生方法。

【請求項８９】使用者を特定するための使用者識別情報が、記録データと共に記録された記録媒体からの前記記録データの再生装置であって、

前記記録媒体からの情報から前記使用者識別情報を検出する使用者識別情報検出手段と、

前記検出した前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致していると検出したときには、前記記録データの再生を許可する制御手段とを備えることを特徴とするデータ再生装置。

【請求項９０】請求項８９に記載のデータ再生装置において、

前記使用者識別情報が予め記憶された不揮発性メモリを備え、

前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とするデータ再生装置。

【請求項９１】請求項８９に記載のデータ再生装置において、

再生装置とは別体の使用者識別情報提供装置からの前記使用者識別情報を取得して、前記不揮発性メモリに記憶するようにする手段を備えることを特徴とするデータ再生装置。

【請求項９２】請求項９１に記載のデータ再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は暗号化されており、前記使用者識別情報の暗号化を解除する手段を備えることを特徴とするデータ再生装置。

【請求項９３】請求項９１に記載のデータ再生装置において、

前記使用者識別情報提供装置からの前記使用者識別情報は、予め前記使用者識別情報提供装置に格納された当該装置ごとに固有の情報であることを特徴とするデータ再生装置。

【請求項９４】請求項８９に記載のデータ再生装置において、

前記記録データは、暗号化されており、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときに、前記暗号化を解除可能とすることを特徴とするデータ再生装置。

【請求項９５】請求項９４に記載のデータ再生装置において、

前記記録データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とするデータ再生装置。

【請求項９６】請求項８９に記載のデータ再生装置において、

前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とするデータ再生装置。

【請求項９７】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ記録再生方法。

【請求項９８】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうことを特徴とするデータ記録再生方法。

【請求項９９】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ記録再生方法。

【請求項１００】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ記録再生方法。

【請求項１０１】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ記録再生方法。

【請求項１０２】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの

情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうことを特徴とするデータ記録再生方法。

【請求項１０３】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可することを特徴とするデータ記録再生方法。

【請求項１０４】請求項１に記載のデータ記録再生方法において、

前記記録データの再生時において、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ記録再生方法。

【請求項１０５】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときに、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうように制御することを特徴とするデータ記録再生装置。

【請求項１０６】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうように制御することを特徴とするデータ記録再生装置。

【請求項１０７】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ記録再生装置。

【請求項１０８】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ記録再生装置。

【請求項１０９】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがって処理を行なうように制御することを特徴とするデータ記録再生装置。

【請求項１１０】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうように制御することを特徴とするデータ記録再生装置。

【請求項１１１】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可するように制御することを特徴とするデータ記録再生装置。

【請求項１１２】請求項２３に記載のデータ記録再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ記録再生装置。

【請求項１１３】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録方法。

【請求項１１４】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記録方法。

【請求項１１５】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、記録を不可とすることを特徴とするデータ記録方法。

【請求項１１６】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録方法。

【請求項１１７】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記

録方法。

【請求項１１８】請求項４５に記載のデータ記録方法において、

前記記録対象データに付随する使用者を特定するための使用者識別情報と、前記使用者識別情報とは別個に用意された使用者識別情報とが一致しなかったときには、記録を不可とすることを特徴とするデータ記録方法。

【請求項１１９】請求項５６に記載のデータ記録装置において、

前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、前記記録対象データに付随して得られる記録条件にしたがった処理を行なうことを特徴とするデータ記録装置。

【請求項１２０】請求項５６に記載のデータ記録装置において、

前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、課金を伴う記録のみを許可することを特徴とするデータ記録装置。

【請求項１２１】請求項５６に記載のデータ記録装置において、

前記制御手段は、前記記録対象データに付随する使用者を特定するための使用者識別情報が検出できなかったときには、記録を不可とすることを特徴とするデータ記録装置。

【請求項１２２】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、前記記録媒体からの情報から抽出される再生条件にしたがって処理を行なうことを特徴とするデータ再生方法。

【請求項１２３】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうことを特徴とするデータ再生方法。

【請求項１２４】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ再生方法。

【請求項１２５】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ再生方法。

【請求項１２６】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうことを特徴とするデータ再生方法。

【請求項１２７】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうことを特徴とするデータ再生方法。

【請求項１２８】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可することを特徴とするデータ再生方法。

【請求項１２９】請求項８１に記載のデータ再生方法において、

前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ再生方法。

【請求項１３０】請求項８９に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときに、前記記録媒体からの情報から抽出される再生条件にしたがった処理を行なうように制御することを特徴とするデータ再生装置。

【請求項１３１】請求項８９に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、制限付きで再生を行なうように制御することを特徴とするデータ再生装置。

【請求項１３２】請求項８９に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、課金を伴う再生のみを許可することを特徴とするデータ再生装置。

【請求項１３３】請求項８９に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から前記使用者識別情報が検出できなかったときには、再生を不可とすることを特徴とするデータ再生装置。

【請求項１３４】請求項８９に記載のデータ再生装置において、

前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、前記記録媒体からの情報から抽出される再生条件にしたがっ

て処理を行なうように制御することを特徴とするデータ再生装置。

【請求項１３５】請求項８９に記載のデータ再生装置において、
前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、制限付きで再生を行なうように制御することを特徴とするデータ再生装置。

【請求項１３６】請求項８９に記載のデータ再生装置において、
前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、課金を伴う再生のみを許可するように制御することを特徴とするデータ再生装置。

【請求項１３７】請求項８９に記載のデータ再生装置において、
前記制御手段は、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致しなかったときは、再生を不可とすることを特徴とするデータ再生装置。

【請求項１３８】記録データと共に、使用者を特定するための使用者識別情報が記録されていることを特徴とする記録媒体。

【請求項１３９】前記使用者識別情報は、前記記録データ中に埋め込まれていることを特徴とする請求項１３８に記載の記録媒体。

【請求項１４０】前記記録データは、前記使用者識別情報に関連付けられた暗号化処理がなされて記録されていることを特徴とする請求項１３８に記載の記録媒体。

【請求項１４１】前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とする請求項１３８に記載の記録媒体。

【請求項１４２】著作権管理を必要とするデータ中に、使用者を特定するための使用者識別情報が含まれてなる伝送データ。

【請求項１４３】前記使用者識別情報は、前記データ中に埋め込まれていることを特徴とする請求項１４２に記載の伝送データ。

【請求項１４４】前記データは、前記使用者識別情報に関連付けられた暗号化処理がなされていることを特徴とする請求項１４２に記載の伝送データ。

【請求項１４５】使用者を特定するための使用者識別情報を含む伝送データを伝送し、
前記伝送データの受信時に、前記伝送データから前記使用者識別情報を検出し、その検出した前記使用者識別情報と、前記伝送データ以外から取得した前記使用者識別情報とを比較し、一致したときに、前記伝送データを利用可能とすることを特徴とするデータ伝送方法。

【請求項１４６】前記使用者識別情報は、前記伝送データ中に埋め込まれていることを特徴とする請求項１４５に記載のデータ伝送方法。

【請求項１４７】前記伝送データは、暗号化されており、前記使用者識別情報と、前記伝送データ以外から取得した前記使用者識別情報とが一致したときに、前記暗号化解除可能とすることを特徴とする請求項１４５に記載のデータ伝送方法。

【請求項１４８】前記伝送データの暗号化は、前記使用者識別情報に関連付けられていることを特徴とする請求項１４７に記載のデータ伝送方法。

【請求項１４９】前記使用者識別情報は、指紋、声紋、脈などの生体情報であることを特徴とする請求項１４５に記載のデータ伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、著作権管理が必要なコンテンツデータ、例えば、オーディオ情報、画像情報、ゲームプログラムおよびデータ、コンピュータプログラムなどのデータを記録、再生する方法、装置に関する。

【０００２】

【従来の技術】デジタルコンテンツの普及に伴い、このデジタルコンテンツについての不正な複製（コピー）による著作権侵害が問題となっている。すなわち、テープ媒体などへのアナログ記録の場合には、オーディオデータや画像データがアナログ的に記録されるため、複製を行なうと品質が劣化する。これに対し、デジタル的にオーディオデータや画像データを記録し再生する機器においては、原理的に複製によって情報品質が劣化することがなく、複製を多数回繰り返すことさえも品質の劣化無しに可能である。

【０００３】そのため、デジタル的に処理を行なう機器による不正コピーによる損害は、アナログの場合よりさらに大きなものとなり、デジタル的に処理を行なう機器における不正コピー防止は、非常に重要になっている。

【０００４】そこで、この問題に対処するため、デジタルコンテンツに複製制御のための情報を付加し、この付加情報を用いて、不正な複製を防止することが行われている。

【０００５】例えば、この複製の防止のための制御として、オーディオコンテンツについては、１回は複製を認めるが、１回複製されたものからの複製を禁止するＳＣＭＳ（Serial Copy Management System）と呼ばれる世代制限の複製制御方式による著作権保護施策が、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク（登録商標））、ＤＡＴ（デジタルオーディオテープ）などにおいて用いられている。

【０００６】このＳＣＭＳ方式の複製制御方式について、図１３を参照して説明する。

19

【０００７】例えば、ディスク１には、オリジナルソースのオーディオ信号がデジタル記録されている。デジタルオーディオ信号は、ディスク１に、所定の記録フォーマットで記録されており、ＳＣＭＳ方式による１回複製可能を示す付加情報が、例えばデジタル信号中の特定のエリアに記録されている。

【０００８】再生装置２は、ディスク１から読み出した信号からデジタルオーディオ信号を再生し、前記の付加情報と共に、記録装置３に伝送する。再生装置２では、通常再生速度（１倍速）に等しい時間分をかけて、デジタルオーディオ信号を記録装置３に伝送する。

【０００９】このデジタルオーディオ信号を受け取った記録装置３は、デジタルオーディオ信号の付加情報が１回複製可能であるときには、入力デジタル信号の複製が可能であると認識する。記録装置３は、付加情報が１回複製可能であることを確認すると、記録可能なディスク４にデジタル信号を複製記録する。その際に、記録装置３は、付加情報を「１回複製可能」の状態から、「複製禁止」の状態に書き換える。したがって、ディスク４には、デジタル信号が複製記録が行われると共に、その付加情報として、「複製禁止」の情報が記録される。

【００１０】この１回目の複製記録が行われたディスク４（第１世代のディスク）が再生装置５で再生されて、記録装置６に供給された場合、記録装置６では、付加情報が「複製禁止」となっていることを検知するので、記録可能なディスク７への記録はできなくなる。

【００１１】このときの複製速度は、再生装置２からのオーディオ信号の伝送速度と等しくなり、オーディオ信号を標準再生時間で再生するとき、すなわち、ノーマル再生速度に等しい速度となる。

【００１２】ここで、標準再生時間とは、オーディオ信号の場合、実時間再生速度であり、人間が通常知覚するときの再生速度である。例えば、データの場合、標準再生速度は各再生機器により決定され、人間の知覚に関わるものではない。

【００１３】以上のようにして、ＳＣＭＳ方式では、記録装置で第１世代の複製は許可するが、第１世代の媒体からの第２世代の複製はできないように制御して、著作権保護を行っている。

【００１４】

【発明が解決しようとする課題】ＳＣＭＳ方式の本来の趣旨は、第２世代の複製を禁止することにより、業としての大量の複製が行なわれてしまうのを防止することにあり、現在、一般化している「個人使用の範囲内での複製は自由」という著作権についての概念を否定するものではない。

【００１５】ところで、最近は、ＭＤ（ミニディスク（登録商標））プレーヤや、カード型メモリプレーヤなどのように、記録再生メディアとして種々のものが登場しており、ユーザも、その日の気分によって、再生メディアとして、ＭＤを用いたり、カード型メモリを用いたりするようになっている。このような現状では複製が頻繁に行なわれるようになるが、常にオリジナルのメディアからしか複製をすることができないＳＣＭＳ方式では、個人使用の範囲内での複製であるにもかかわらず、不便を来たしてしまう。

20

【００１６】また、最近のパーソナルコンピュータは、ＣＤプレーヤの機能を備え、ハードディスクにＣＤの音楽情報を格納（複製）して再生できるようになっている。カード型メモリへの複製は、複製速度が速いことから、パーソナルコンピュータのハードディスクからの複製が便利であるが、厳密には、ハードディスクからの複製は、第２世代になり、その複製はできないことになる。

【００１７】この発明は、以上の点にかんがみ、ＳＣＭＳ方式を採用することなく、個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止することができる方法および装置を提供することを目的とする。

【００１８】

【課題を解決するための手段】上記課題を解決するため、請求項１の発明によるデータ記録再生方法は、記録データの記録時には、使用者を特定するための使用者識別情報を、前記記録データと共に、記録媒体に記録し、前記記録データの再生時には、前記記録媒体からの情報から検出された前記使用者識別情報と、前記記録媒体以外から取得した前記使用者識別情報とが一致したときは、前記記録データの再生を許可することを特徴とする。

【００１９】上記の請求項１の発明によれば、使用者識別情報が、記録データと共に、記録媒体に記録されている。そして、再生時には、記録媒体からの情報から検出された使用者識別情報が、記録媒体以外から取得した前記使用者識別情報と比較され、一致したときには、その記録データは、その再生装置の使用者が所有しているものであるとして認識され、再生可能とされる。

【００２０】したがって、個人使用の範囲内での複製が自由になると共に、業として不正な複製が行なわれたときには、その複製により作成された記録媒体からの情報から検出された使用者識別情報と、再生装置の使用者の使用者識別情報とが再生時に不一致になることから、再生ができなくなり、業としての不正な複製を実質的に防止することができる。

【００２１】また、請求項５の発明は、請求項１に記載のデータ記録再生方法において、前記記録データの記録時には、記録装置とは別体の使用者識別情報提供装置から、前記使用者識別情報を前記記録装置に供給するようにし、前記使用者識別情報提供装置が前記記録装置に接続されていないときには、前記記録データの記録を不可とすることを特徴とする。

【００２２】この請求項５の発明によれば、使用者識別情報提供装置が記録装置に接続されていないときには、記録ができないようにされているので、記録時には、必ず、記録データと共に、使用者識別情報が記録媒体に記録される。したがって、再生時の、使用者識別情報を用いた再生制御と相俟って、個人使用の範囲内の複製にとどめることができる。

【００２３】さらに請求項６の発明は、請求項５に記載のデータ記録再生方法において、前記使用者識別情報が予め記憶された不揮発性メモリを設け、前記不揮発性メモリから読み出した前記使用者識別情報を、前記記録媒体以外から取得した前記使用者識別情報とすることを特徴とする。

【００２４】この請求項６の発明によれば、請求項５の要件により、記録時に記録データと共に使用者識別情報が記録媒体に確実に記録されて、使用者の制限が厳格に行われる代わりに、再生側では、不揮発性メモリに予め登録した使用者識別情報を用いて、記録媒体からの使用者識別情報と比較することができる。したがって、使用者は、再生時には、記録時のような使用者識別情報提供装置を、再生装置に接続しなくても再生出力を得ることができ、使い勝手がよくなる。

【００２５】

【発明の実施の形態】以下、この発明によるデータ記録・再生方法および装置の実施の形態を、ディスク記録媒体にオーディオ信号を記録し、再生する場合を例にとって、図を参照しながら説明する。

【００２６】図１は、この発明によるデータ記録再生装置の第１の実施の形態を用いた記録再生システムのブロック図である。

【００２７】この第１の実施の形態のシステムにおいては、図１に示すように、実施の形態のデータ記録再生装置１０と、使用者識別情報提供装置２０とからなる。使用者識別情報提供装置は、以下の説明においては、ユーザＩＤモジュールと称する。この実施の形態においては、データ記録再生装置１０には、ユーザＩＤモジュール２０を接続するための端子が、必ず付いている。この端子を通じて、データ記録再生装置１０とユーザＩＤモジュール２０との間でやり取りする情報は、すべて暗号化される。

【００２８】データ記録再生装置１０は、記録再生用信号処理部（以下、記録再生エンジンチップと称する）１１と、記録／再生装置部１２と、システム制御部１３と、不揮発性メモリ１４と、入力操作部１５と、表示部１６とを備えている。記録再生エンジンチップ１１は、機能的には、記録エンコード／再生デコード処理部１１１と、ユーザＩＤモジュール２０との間で、暗号化を伴う通信パスを確立して通信を行なうための暗号処理部１１２と、制御部１１３とを備えて構成されている。

【００２９】そして、記録再生エンジンチップ１１の記録エンコード／再生デコード処理部１１１は、システム制御部１３の制御を受けて、記録時には、これに対して入力されるアナログオーディオ信号あるいはデジタルオーディオ信号を、後述のように記録エンコード処理して、記録／再生装置部１２に出力し、また、再生時には、記録／再生装置部１２からの再生データを後述のように再生デコードして、アナログオーディオ信号あるいはデジタルオーディオ信号として出力する。

【００３０】また、記録再生エンジンチップ１１の暗号化処理部１１２は、ユーザＩＤモジュール２０に対して、この例では、ケーブル４０を通じて接続される。この場合、暗号化処理部１１２は、システム制御部１３の制御の下、ユーザＩＤモジュール２０との間で認証作業を行う認証機能を備え、認証がとれたときに、ユーザＩＤモジュール２０との間に通信路を確立する。この場合に、確立した通信路を伝送するデータは暗号化するものであるので、通信を行なう前に、その暗号化および暗号解除のための暗号鍵の伝達を行なう。

【００３１】また、記録再生エンジンチップ１１の制御部１１３は、システム制御部１３からの制御信号に応じて記録エンコード／再生デコード処理部１１１と、暗号処理部１１２を動作制御すると共に、この制御部１１３に対して接続される不揮発性メモリ１４に対する使用者識別情報の、書き込み、読み出しを制御する。

【００３２】記録／再生装置部１２は、システム制御部１３による制御を受けて、記録再生エンジンチップ１１からの記録信号を、ディスク３０に記録し、また、ディスク３０から読み出したデータを、記録再生エンジンチップ１１に供給する。

【００３３】システム制御部１３は、入力操作部１５を通じた使用者の入力指示に従った制御を行ない、また、必要な表示用データを表示部１６に送って、その画面に表示する。表示部１６の表示素子としては、液晶ディスプレイなどが用いられる。

【００３４】ユーザＩＤモジュール２０は、一つのデータ記録再生装置１０に、一つ付属するもので、使用者識別情報（以下、ユーザＩＤという）をデータ記録再生装置１０に供給するものである。ユーザＩＤモジュール２０は、暗号処理および制御部（以下、セキュアチップと称する）２１と、不揮発性メモリ２２と、入力操作部２３と、表示部２４とを備えて構成されている。

【００３５】セキュアチップ２１は、記録再生エンジンチップ１１との間で認証作業を行う機能を備え、認証がとれたときに、記録再生エンジンチップ１１との間に通信路を確立する。この際に、通信路を伝送するデータは暗号化するものであるので、通信を行なう前に、暗号化および暗号解除のための暗号鍵の伝達を行なう。

【００３６】不揮発性メモリ２２には、予め工場出荷時に、各ユーザＩＤモジュール２０に固有のモジュール識別情報（以下、モジュールＩＤと称する）、例えば固有

の数値が書き込まれている。

【００３７】そして、使用者は、データ記録再生装置１０を購入したときに、それに付属しているユーザＩＤモジュール２０に、入力操作部２３を通じて、表示部２４の画面で確認しながら、「ユーザ名」を入力して登録する。

【００３８】［ユーザＩＤモジュール２０へのユーザ名の登録］図２は、このユーザＩＤモジュール２０への「ユーザ名」の登録のための処理手順を示すフローチャートである。

【００３９】先ず、ユーザＩＤモジュール２０は、「ユーザ名」の入力するための画面を、表示部２４に表示し、使用者に、ユーザＩＤモジュール２０への「ユーザ名」の入力を促す（ステップＳ１）。これを受けて、使用者が、ユーザ名を入力すると、ユーザＩＤモジュール２０は、そのユーザ名の入力完了を確認した後（ステップＳ２）、入力された「ユーザ名」を、不揮発性メモリ２２に格納する。以上の処理は、セキュアチップ２１が実行するものである。

【００４０】なお、以上のようにして入力されて登録されたユーザ名は、入力操作部２３を通じた登録ユーザ名の確認操作が行なわれたときに、不揮発性メモリ２２から読み出されて、表示部２４の画面に表示されて、確認することができるようにされている。

【００４１】こうして、入力された「ユーザ名」と、不揮発性メモリ２２に予め記憶されていた「モジュールＩＤ」とが、１対１に対応付けられることにより、実質的にモジュールＩＤがユーザＩＤとしての意味を有することになる。つまり、ユーザＩＤは、この明細書においては、モジュールＩＤとユーザ名との両方を含む概念を意味する場合と、モジュールＩＤのみからなる概念を意味する場合の２通りの場合がある。

【００４２】［データ記録再生装置へのユーザＩＤの登録］以上のようにして、ユーザ名がユーザＩＤモジュール２０に登録された後には、使用者は、ユーザＩＤモジュール２０をデータ記録再生装置１０に接続して、データ記録再生装置１０に対するユーザＩＤ登録を行なう必要がある。

【００４３】図３および図４は、ユーザＩＤモジュール２０を用いて、データ記録再生装置１０にユーザＩＤの登録をする処理手順を示すフローチャートである。図３は、このときの、ユーザＩＤモジュール２０側での処理であり、また、図４は、データ記録再生装置１０側での処理である。

【００４４】＜ユーザＩＤモジュール２０側の処理動作＞ユーザＩＤモジュール２０では、図３に示すように、先ず、データ記録再生装置１０に接続されたかどうか判別する（ステップＳ１１）。接続されていないと判別されたときには、データ記録再生装置１０が接続されていないことを使用者に報知して、接続を促すようにする（ステップＳ１２）。

【００４５】そして、データ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、使用者による入力操作部２３を通じた「登録指示」を待ち（ステップＳ１３）、登録指示が受け付けられたことを検知したときには、データ記録再生装置１０の記録再生エンジンチップ１１との間での認証確認すると共に、暗号鍵の伝達を行なう（ステップＳ１４）。

【００４６】そして、認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ１５）、認証ができずに、通信路が確立できなかったときには、表示部２４にエラー表示をして（ステップＳ１７）、この処理ルーチンを終了する。また、通信路が確立できたときには、不揮発性メモリ２２からモジュールＩＤおよびユーザ名を読み出し、暗号化して、データ記録再生装置１０に対して、登録命令と共に送信する（ステップＳ１６）。

【００４７】＜データ記録再生装置１０側の処理動作＞一方、データ記録再生装置１０側においては、図４に示すように、先ず、ユーザＩＤモジュール２０が接続されるのを待ち、接続されたことを判別すると（ステップＳ２１）、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０との間での認証確認すると共に、暗号鍵の伝達を行なう（ステップＳ２２）。

【００４８】そして、認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ２３）、認証ができずに、通信路が確立できなかったときには、表示部１６にエラー表示をして（ステップＳ２６）、この処理ルーチンを終了する。

【００４９】また、通信路が確立できたときには、ユーザＩＤモジュール２０からの「モジュールＩＤ」および「ユーザ名」を含む登録命令の受信を待ち（ステップＳ２４）、受信を確認したら、記録再生エンジンチップ１１は、不揮発性メモリ１４に、受信したモジュールＩＤおよびユーザ名を格納して、所有者登録をする（ステップＳ２５）。

【００５０】なお、以上のようにして入力されて登録されたユーザ名は、入力操作部１５を通じた登録ユーザ名の確認操作が行なわれたときに、不揮発性メモリ１４から読み出されて、表示部１６の画面に表示されて、確認することができるようにされている。

【００５１】また、データ記録再生装置１０のユーザＩＤは、一旦登録されたものであっても、ユーザＩＤモジュール２０を用いて再登録することにより、別のユーザＩＤに設定し直すこともできる。

【００５２】［データ記録再生装置１０での録音処理動作］次に、データ記録再生装置１０での録音処理動作を図５および図６のフローチャートを参照しながら説明する。

【００５３】この実施の形態においては、録音をする際には、データ記録再生装置１０には、ユーザＩＤモジュ

ール２０を接続しておく必要がある。すなわち、データ記録再生装置１０は、先ず、ユーザＩＤモジュール２０が接続されているかどうか判別する（ステップＳ３１）。接続されていないと判別されたときには、ユーザＩＤモジュール２０が接続されていないことを使用者に報知して、接続を促すようにする（ステップＳ３２）。例えば「ユーザＩＤモジュールが接続されていないので記録はできません。ユーザＩＤモジュールを接続して下さい。」というメッセージを表示部１６に表示したり、音声によるメッセージとして放音するようにする。

【００５４】そして、データ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、使用者による入力操作部１５を通じた「録音指示」を待ち（ステップＳ３３）、「録音指示」が受け付けられたことを検知したときには、データ記録再生装置１０のシステム制御部１３は、録音命令を記録再生エンジンチップ１１や記録／再生装置部１２に発行し、録音開始準備状態とする（ステップＳ３４）。

【００５５】次に、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０のセキュアチップ２１との間での認証確認すると共に、暗号鍵の伝達を行なう（ステップＳ３５）。そして、認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ３６）、認証ができずに、通信路が確立できなかったときには、録音動作を中止し（ステップＳ３７）、その後、表示部２４にエラー表示をして（ステップＳ３８）、この処理ルーチンを終了する。

【００５６】また、ステップＳ３６で、通信路が確立できたと判別したときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０に対して、ユーザＩＤ、つまり、この例の場合には、モジュールＩＤおよびユーザ名の送信要求を出す（ステップＳ３９）。

【００５７】ユーザＩＤモジュール２０のセキュアチップ２１は、この送信要求に対して、不揮発性メモリ２２からモジュールＩＤおよびユーザ名を読み出し、暗号化して、データ記録再生装置１０に対して送信する。データ記録再生装置１０の記録再生エンジンチップ１１は、このモジュールＩＤおよびユーザ名の受信を確認する（ステップＳ４０）。

【００５８】次に、オーディオデータ中に埋め込まれているモジュールＩＤの検出を行ない（ステップＳ４１）、モジュールＩＤが検出できたか否か判別する（ステップＳ４２）。そして、モジュールＩＤが検出できたときには、検出されたモジュールＩＤと、ユーザＩＤモジュール２０から取得したモジュールＩＤとを比較照合する（ステップＳ４３）。

【００５９】その比較照合の結果、両モジュールＩＤが一致したか否か判別し（ステップＳ４４）、一致したときには、記録許可となり、入力オーディオデータを圧縮し、受信したユーザＩＤを暗号鍵とした暗号化処理する（ステップＳ４５）。

【００６０】この場合、暗号鍵としては、ユーザ名のみを用いる場合、モジュールＩＤのみを用いる場合、またはユーザ名およびモジュールＩＤの両者を用いる場合のいずれであってもよい。

【００６１】そして、この圧縮および暗号化処理したオーディオデータ中に、ユーザＩＤモジュール２０から取得した「ユーザ名」と、「モジュールＩＤ」とを埋め込む（ステップＳ４６）。この場合に、モジュールＩＤは暗号化して埋め込む。ユーザＩＤの秘匿性を高めるためである。ステップＳ４６では、さらに、後述する記録ルールや再生ルールを、記録対象のオーディオデータに埋め込む。

【００６２】以上のようにして、暗号化し、ユーザＩＤなどを埋め込んだオーディオデータは、記録媒体としてのディスク３０に記録する（ステップＳ４７）。

【００６３】一方、ステップＳ４２でモジュールＩＤが検出できなかったときと、ステップＳ４４でオーディオデータから検出されたモジュールＩＤとユーザＩＤモジュール２０からのモジュールＩＤとが不一致であったときには、オーディオデータ中に埋め込まれている記録条件（記録ルール）を検出し（ステップＳ４８）、その検出した記録ルールにしたがった処理を行なう（ステップＳ４９）。

【００６４】この記録ルールの情報の埋め込み処理としては、電子透かし処理と呼ばれている処理や、その他の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、ＴＯＣ（Ｔａｂｌｅ Ｏｆ Ｃｏｎｔｅｎｔｓ）などのオーディオデータとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

【００６５】このとき埋め込む記録ルールとしては、例えば、

Ｒ①「無料で記録（複製）可能」
Ｒ②「記録（複製）は有料」
Ｒ③「記録（複製）はフリー」
Ｒ④「記録（複製）は不可」

のうちの一つが選択されて記録されているものである。記録ルールの記録情報としては、記録ルールの内容そのものを記録してもよいが、上述のＲ①～Ｒ④のいずれであるかの情報を記録することもできる。

【００６６】ここで、上記Ｒ①「無料で記録（複製）可能」は、ユーザＩＤをオーディオデータに埋め込んで、記録を実行させるものである。これは、この例では、オーサリング装置でレコード会社などにより制作される読み出し専用形式（以下、ＲＯＭタイプという）のディスクなどの記録媒体には、所有者無しとしてユーザＩＤを埋め込まずに記録するので、このＲＯＭタイプの記録媒体からのオーディオデータの記録（複製）時の処理となる。

【００６７】また、上記R②「記録（複製）は有料」は、課金処理が可能な記録装置において、課金処理が実行できたときに記録を許可するものである。課金処理が不能の記録装置の場合には、記録は不可とされる。なお、課金処理の例については、後述する。

【００６８】また、上記R③「記録（複製）はフリー」は、ユーザＩＤはオーディオデータに記録せずに、記録（複製）を行なう処理である。さらに、R④「記録（複製）は不可」は、全く記録（複製）は不可であることを意味している。

【００６９】なお、上述のように、記録ルールは、ユーザＩＤが不一致の場合だけでなく、記録対象のオーディオデータからユーザＩＤが検出できなかったときにも適用されるが、ユーザＩＤが不一致の場合と、有効なユーザＩＤが得られない場合とでは、異なる記録ルールを記録しておくようにしてもよい。

【００７０】また、後述するように、この実施の形態では、再生時には、オーディオデータ中に埋め込まれたユーザＩＤと、不揮発性メモリ１４に格納されたユーザＩＤとの照合を行ない、両者が一致したときに、そのオーディオデータの再生が可能となる。そして、この実施の形態では、再生時にオーディオデータからユーザＩＤが検出できなかったとき、また、再生時での照合の結果、ユーザＩＤが不一致であるときに、どのように処理するかの再生ルール（再生条件）も、ステップＳ４６で、オーディオデータ中に埋め込むようにする。

【００７１】この再生ルールの情報の埋め込み処理としては、記録ルールと同様に、電子透かし処理と呼ばれている処理や、その他の周知の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、ＴＯＣ（ＴａｂｌｅＯｆ　Ｃｏｎｔｅｎｔｓ）などのオーディオデータとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

【００７２】この再生時にユーザＩＤが不一致の場合の再生ルールとしては、例えば、

ＰＢ①「無料再生可能」
ＰＢ②「再生禁止（再生不可）」
ＰＢ③「再生は有料」
ＰＢ④「制限付きで再生可能」

のうちの一つが選択されて記録されるものである。再生ルールの記録情報としては、再生ルールの内容そのものを記録してもよいが、上述のＰＢ①～ＰＢ④のいずれであるかの情報を記録することもできる。

【００７３】ここで、上記ＰＢ①「無料再生可能」の場合には、再生装置に登録されたユーザＩＤに関係なく、常に、再生可能可能となり、ＰＢ②「再生禁止（再生不可）」の場合には、再生装置に登録されたユーザＩＤに関係なく、常に、再生が禁止される。前述したように、この例では、オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体には、ユーザＩＤを埋め込まずに記録するので、再生オーディオデータから有効なユーザＩＤが得られない場合として、上記ＰＢ①のルールが記録される。

【００７４】また、上記ＰＢ③「再生は有料」の場合には、課金処理が可能な再生装置において、課金処理が実行できたときに再生を許可するものである。課金処理が不能の再生装置の場合には、再生は不可とされる。なお、課金処理の例については、後述する。

【００７５】また、上記ＰＢ④「制限付きで再生可能」は、例えば、全部又は一部の試聴モードを許可し、その試聴モードの後は、上記ＰＢ②又はＰＢ③のルールとするものである。ここで、試聴モードとは、

ａ）ｎ回、例えば１回だけ無料再生可能
ｂ）ｍ秒分だけ無料再生可能
ｃ）さわり部分やさび部分だけ無料再生可能

を意味する。

【００７６】このＰＢ④「制限付き再生可能」の再生ルールで、前記ａ）やｂ）を採用する場合には、再生装置は、例えば、ＩＳＲＣ（ＩｎｔｅｒｎａｔｉｏｎａｌＳｔａｎｄａｒｄ　Ｒｅｃｏｒｄｉｎｇ　Ｃｏｄｅ）などのコンテンツＩＤ（識別コード）に対応させて、そのコンテンツＩＤで識別されるオーディオデータの試聴履歴の情報、例えば試聴回数や、試聴秒数などを記録するようにする。

【００７７】この実施の形態では、後述の再生処理で説明するように、この再生ルールは、再生時にユーザＩＤが不一致の場合だけでなく、再生オーディオデータから、有効なユーザＩＤが得られないときにも共通に適用される。しかし、ユーザＩＤが不一致の場合と、有効なユーザＩＤが得られない場合とでは、異なる再生ルールを記録するようにしてもよい。

【００７８】例えば、オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体にも、ユーザＩＤとして、例えば「ＯＲＩＧＩＮＡＬ」などの特定のＩＤが記録される場合には、再生装置は、その特定のＩＤを検出したときには、自己の装置のユーザＩＤと不一致の場合でも、再生許可すべきである。したがって、再生ルールが埋め込まれるものとした場合には、その再生ルールは、「再生可能」とされる。

【００７９】一方、このように特定のユーザＩＤが、ＲＯＭタイプのディスクなどの記録媒体の記録データに埋め込まれるなどして、前記記録データに付随して記録されると定められている場合には、再生装置において、有効なユーザＩＤが得られないときには、そのオーディオデータは、不正に記録されたものであるとすることができる。したがって、その時の再生ルールは再生不可とするのがよい。

【００８０】しかし、オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体には、ユーザＩＤを記録しないと定められている

場合には、上述のような再生ルールのうちの一つを共通に用いることができる。

【００８１】［データ記録再生装置１０での再生処理動作］次に、以上のようにして録音されたオーディオデータを、データ記録再生装置１０で再生する場合の処理動作を図７および図８のフローチャートを参照しながら説明する。

【００８２】先ず、記録済みのディスクが装填されるのを待ち、装填されたことを判別すると（ステップＳ５１）、記録再生エンジンチップ１１は、使用者からの再生指示を待つ。そして、使用者からの再生指示を確認すると（ステップＳ５２）、ディスクから再生指示のあったオーディオデータを読み出す（ステップＳ５３）。

【００８３】そして、読み出されたオーディオデータに埋め込まれているユーザＩＤを検出する。そして、ユーザＩＤのうちの、この例では、暗号化されているモジュールＩＤの暗号を解除して検出する（ステップＳ５４）。そして、モジュールＩＤが検出できたか否か判別し（ステップＳ５５）、検出できなかったときには、再生オーディオデータに埋め込まれている再生ルールを検出し（ステップＳ７３）、その検出された再生ルールに従った処理を行なう（ステップＳ７４）。

【００８４】また、ステップＳ５５で、モジュールＩＤを検出することができたと判別されたときには、その検出されたモジュールＩＤと、不揮発性メモリ１４に記憶されているモジュールＩＤとを比較照合する（ステップＳ５６）。

【００８５】そして、両者が一致しているかどうか判別し（ステップＳ５７）、一致しているときには、ユーザＩＤが用いられて暗号化されているオーディオデータの暗号を解き（ステップＳ５８）、また、オーディオデータの圧縮を解凍する（ステップＳ５９）。そして、オーディオデータを復号して、再生出力する（ステップＳ６０）。

【００８６】一方、ステップＳ５７で、ディスク３０から読み出したデータから検出されたモジュールＩＤと、不揮発性メモリ１４から読み出されたモジュールＩＤとが不一致であると判別されたときには、ユーザに、ユーザＩＤモジュール２０を接続させる設定になっているかどうかを判別し、ユーザＩＤモジュールを接続させる設定になっていなければ、再生オーディオデータに埋め込まれている再生ルールを検出し（ステップＳ７３）、その検出された再生ルールに従った処理を行なう（ステップＳ７４）。この例では、例えば再生禁止となる。

【００８７】この場合の再生禁止には、正常な再生出力が行なわれないことも含まれる。つまり、再生出力としてノイズが出力される場合の他、再生出力に代えて、「違法に複製された記録媒体からの再生である」旨のメッセージを、オーディオ出力として送出するようにしてもよい。

【００８８】ステップＳ６１で、ユーザに、ユーザＩＤモジュールを接続させる設定になっていると判別されたときには、データ記録再生装置１０は、ユーザＩＤモジュール２０が接続されているかどうか判別する（ステップＳ６２）。接続されていないと判別されたときには、ユーザＩＤモジュール２０が接続されていないことを使用者に報知して、接続を促すようにする（ステップＳ６３）。

【００８９】そして、データ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０との間での認証確認すると共に、暗号鍵の伝達を行なう（ステップＳ６４）。そして、認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ６５）、認証ができずに、通信路が確立できなかったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行なう（ステップＳ７３、ステップＳ７４）。この例では、前述のように再生禁止となる。

【００９０】また、ステップＳ６５で、通信路が確立できたと判別したときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０に対して、ユーザＩＤのうちの、この例の場合には、モジュールＩＤの送信要求を出す（ステップＳ６６）。

【００９１】ユーザＩＤモジュール２０のセキュアチップ２１は、この送信要求に対して、不揮発性メモリ２２からモジュールＩＤを読み出し、暗号化して、データ記録再生装置１０に対して送信する。データ記録再生装置１０の記録再生エンジンチップ１１は、このモジュールＩＤの受信を確認すると（ステップＳ６７）、ディスク３０から読み出したデータから検出されたモジュールＩＤと、受信し暗号を解除したモジュールＩＤとを比較照合する（ステップＳ６８）。

【００９２】そして、両者が一致しているかどうか判別し（ステップＳ６９）、両者が不一致であったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行なう（ステップＳ７３、ステップＳ７４）。前述したように、この例では、再生禁止となる。

【００９３】また、両者が一致したときには、ユーザＩＤが用いられて暗号化されているオーディオデータの暗号を解き（ステップＳ７０）、また、オーディオデータの圧縮を解凍する（ステップＳ７１）。そして、オーディオデータを復号して、再生出力する（ステップＳ７２）。

【００９４】以上のようにして、この実施の形態においては、記録時に、登録されたユーザＩＤを記録データに埋め込んで記録し、再生時には、不揮発性メモリ１４に登録されたユーザＩＤと、ディスク３０から読み出されたデータから検出されたユーザＩＤとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にする

ことができる。

【００９５】また、上述の実施の形態では、記録時には、ユーザＩＤモジュール２０を、データ記録再生装置１０に接続した状態ではないと記録を実行することができないようにしたので、この点でも、ユーザの個人使用の範囲内での制限をすることができる。

【００９６】そして、この実施の形態では、記録側に上記のような制限を加えた代わりに、再生側においては、不揮発性メモリ１４に登録されたユーザＩＤと、ディスク３０から読み出されたデータから検出されたユーザＩＤとを比較して、両者が一致しているかどうかを判別するようにしており、記録時のように、ユーザＩＤモジュール２０を接続する必要はなく、再生時におけるユーザの使い勝手が良くなるという効果がある。

【００９７】例えば、「個人使用の範囲でコピーは自由」ということを具現化する方法として、個人で取得済みの聴取権情報（例えば、その個人が持っているコンテンツのすべての情報）を自分専用のＩＣカードに記録しておき、コンテンツを再生する際には、必ずそのＩＣカードを再生装置に差し込むようにする方法が考えられる。この場合、ＩＣカードを他人が使えない状態に保つために、一人一枚のＩＣカードを持つように管理される。

【００９８】このようにすれば、ＩＣカードが、その個人のすべての聴取権情報を持つので、コンテンツの複製は、全く自由にしてしまっても問題がなくなるが、その代わりに、使用者は、再生装置に差し込むＩＣカードを持ち歩かなければならなくなるという問題がある。

【００９９】しかし、上述の実施の形態の場合には、再生装置には、そのＩＣカードのようなものは不要となるので、非常に便利である。

【０１００】また、上述の実施の形態では、記録データは、ユーザＩＤを暗号鍵とした暗号を施して記録するようにしているので、再生時には、ユーザＩＤが一致したときにしか、記録データの暗号化が解除できなくなり、より個人使用の範囲内での制限を確実にすることができる。

【０１０１】なお、ユーザＩＤを暗号鍵そのものとせず、記録データの暗号化の鍵を取得するための情報などのように、暗号化に関連する情報として用いても、同様の効果が得られると期待できる。

【０１０２】また、上述の実施の形態では、ユーザＩＤモジュール２０からのユーザＩＤの情報は、暗号化してデータ記録再生装置１０に送るようにしており、このため、ユーザＩＤの秘匿性を高めることができるという効果もある。

【０１０３】なお、上述の説明では、記録ルールおよび再生ルールをオーディオデータに埋め込んだので、記録ルールおよび再生ルールの情報は、オーディオデータから検出するようにするが、記録ルールおよび再生ルールの情報が、ＴＯＣなどに記録されていた場合には、記録対象のオーディオデータに先立ち、記録ルールおよび再生ルールの情報を取得するようにすればよい。

【０１０４】また、オーディオデータが圧縮されてブロック化されている場合には、ブロックとブロックの間の隙間に記録ルールおよび再生ルールの情報を埋め込むようにすることもできる。その場合には、圧縮デコードのときに、記録ルールおよび再生ルールの情報を抽出することができる。

【０１０５】また、データ記録再生装置１０が、再生と記録が同時にでき、複製記録ができるように、記録媒体を同時に複数枚装填できるようにされている場合には、再生側のディスクから記録ルールや再生ルールの情報を予めＴＯＣや再生データから得るようにすることもできる。

【０１０６】なお、以上の実施の形態では、記録ルールおよび再生ルールをオーディオデータ中に必ず記録するように説明したが、予め、システムとして、ユーザＩＤが得られなかったとき、また、ユーザＩＤが不一致のときの、記録ルールおよび再生ルールを、例えば上述のルールのうちの一つに定めておくようにすれば、記録ルールおよび再生ルールをオーディオデータ中に記録する必要はなくなる。

【０１０７】［第２の実施の形態］この第２の実施の形態は、データ記録再生装置が、パーソナルコンピュータに搭載される場合の例である。図８は、この第２の実施の形態の場合のシステムのブロック図である。

【０１０８】この第２の実施の形態のシステムは、パーソナルコンピュータ５０と、前述の第１の実施の形態の場合に用いたユーザＩＤモジュール２０とにより構成される。

【０１０９】この実施の形態のパーソナルコンピュータ５０は、ユーザＩＤモジュール２０を接続するための端子を備えている。そして、この端子を通じて、ユーザＩＤモジュール２０との間でやり取りする情報は、すべて暗号化されるものである。

【０１１０】パーソナルコンピュータ５０は、第１の実施の形態のデータ記録再生装置１０と同様に、記録再生エンジン５１と、記録／再生装置部５２と、不揮発性メモリ５４とを備えると共に、システムバス５９を介して、ＣＰＵ５３と、入力操作部５５と、表示部５６と、ネットワークインターフェース５７と、ハードディスク装置５８とが接続される。システムバス５９には、記録再生エンジン５１と、記録／再生装置部５２も接続されている。

【０１１１】そして、ネットワークインターフェース５７は、ネットワーク６０に接続された記憶装置６１に対して接続される。ここで、ネットワーク６０は、ローカルエリアネットワーク（ＬＡＮ）であっても良いし、インターネットであってもよい。インターネットの場合に

は、記憶装置６１は、所定のサーバなどに設けられた記録装置とされる。

【０１１２】この第２の実施の形態においても、前述の第１の実施の形態と全く同様にして、ユーザＩＤモジュール２０には、ユーザ名が入力登録され、その後、パーソナルコンピュータ５０にユーザＩＤの登録処理が、ユーザＩＤモジュール２０から、パーソナルコンピュータ５０に対して行われて、不揮発性メモリ５４には、ユーザＩＤが登録されて記憶される。

【０１１３】そして、この第２の実施の形態の場合には、記録メディアとしては、第１の実施の形態の場合のディスク３０のみではなく、ハードディスク装置５８やネットワーク６０に接続された記憶装置１６も用いられる。

【０１１４】すなわち、この第２の実施の形態の場合の記録における入力ソースと、記録媒体（記録メディア）との組み合わせを示すと、

①アナログ入力あるいはデジタル入力→ディスク３０
②アナログ入力あるいはデジタル入力→ハードディスク装置５８
③アナログ入力あるいはデジタル入力→記憶装置６１
④ディスク３０→ハードディスク装置５８
⑤ディスク３０→記憶装置６１
⑥ハードディスク装置５８→ディスク３０
⑦ハードディスク装置５８→記憶装置６１
⑧記憶装置６１→ディスク３０
⑨記憶装置６１→ハードディスク装置５８

などがある。

【０１１５】この９通りの他にも、ネットワーク６０上の一つの記憶装置から、他の記憶装置に転送して書き込む処理も、記録処理の一つと考えられる。以上のいずれの記録時においても、この第２の実施の形態では、前述の第１の実施の形態と同様にして、ユーザＩＤモジュール２０が接続されることを条件とすると共に、そのユーザＩＤモジュール２０から取得したユーザ名およびモジュールＩＤとを、記録データに埋め込んで記録するようにする。この場合に、第１の実施の形態と同様に、モジュールＩＤは、暗号化して記録するようにする。

【０１１６】この場合、ハードディスク装置５８への記録の場合には、記録再生エンジンチップ１１で記録エンコードされたデータは、記録／再生装置部５２を経ることなく、システムバス５９を通じてハードディスク装置５８に送られて、ハードディスクに格納される。

【０１１７】また、記憶装置６１への記録の場合には、記録再生エンジンチップ１１で記録エンコードされたデータは、記録／再生装置部５２を経ることなく、システムバス５９およびネットワークインターフェース５７を通じて記憶装置６１に対してネットワーク６０に送出され、記憶装置６１に格納されるようにされる。

【０１１８】そして、ディスク３０、ハードディスク装置５８、記憶装置６２のいずれからのオーディオデータの再生時においても、前述の第１の実施の形態と全く同様に、再生データ中から検出したユーザＩＤと、不揮発性メモリ５４に記憶されていたユーザＩＤとの照合が行われて、両者が一致したときに、オーディオデータの再生出力を可能とするようにする。

【０１１９】この第２の実施の形態の場合にも、上述した第１の実施の形態と同様の効果が得られると共に、ハードディスク装置５８を用いた高速複製が、ユーザの個人使用の範囲内という制限を保持して可能となる。また、ネットワークを通じた記憶装置へのデータ転送も、一つの記録（複製）態様とすることができるが、それも、ユーザの個人使用の範囲内という制限を保持して可能となる。

【０１２０】［課金処理の例について］次に、記録ルールおよび再生ルールが課金を条件にしている場合に対応する実施の形態を説明する。図１０は、この例の課金処理システムの一例を示すものであり、音楽コンテンツの配付、音楽コンテンツのデータの授受については、省略されている。この実施の形態のデータ記録再生装置１０は、複製記録ができるように構成されている。つまり、あるディスクからのデータを、別のディスクに記録することが可能とされている。

【０１２１】この実施の形態の場合、課金処理のために、記録に際しては複製権データが、再生に際しては聴取権データが、それぞれ使用される。これら複製権データおよび聴取権データは、ＩＣカードや、データ記録再生装置１０に設けられるセキュアデコーダ１７のメモリに格納される。

【０１２２】複製権データおよび聴取権データは、例えば複製可能な度数および再生可能な度数であり、データ記録再生装置１０が課金対象のコンテンツを記録／再生する度に、それぞれの度数が減算される。

【０１２３】これら複製権データおよび聴取権データは、複製／聴取権データ管理会社の管理下で、ユーザが所有する複製／聴取権データチャージャまたは販売店に設置された複製／聴取権データ販売端末２０５によって書き替えることが可能とされている。この例では、複製／聴取権データチャージャは、ユーザＩＤモジュール２０内に課金データチャージャ２５として設けられている。

【０１２４】課金データチャージャ２５は、データ記録再生装置１０のセキュアデコーダ１７と決済センター２０３またはレコード店、コンビニエンスストア等に設置されているデータ販売端末２０５との間に存在して聴取権データ中継器として機能する。

【０１２５】また、レコード会社２０１、著作権管理機構２０２、ユーザデバイスとしてのデータ記録再生装置１０と関係して、代金決済のために、決済センター２０３が存在している。決済センター２０３は、認証／課金

サーバを備えている。決済センター２０３は、銀行、クレジットカード会社２０４との間で代金の決済を行なう。

【０１２６】図１０において、破線で示すように、レコード会社２０１から配布される、記録再生装置１０が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、この他、種々のものが使用できる。また、記録再生装置１０は音楽コンテンツを媒体（光ディスク、メモリカード等）３０に記録する。

【０１２７】データ記録再生装置１０内のセキュアデコーダ１７と、課金データチャージャ２５とが、この例では有線の通信路を介して通信を行い、複製／聴取権データが課金データチャージャ２５からセキュアデコーダ１７内のメモリに対して転送される。複製／聴取権データは、例えばデータ記録再生装置１０の、記録（複製）可能回数または記録（複製）可能時間／再生可能回数情報または再生可能時間に対応している。

【０１２８】また、データ記録再生装置１０のセキュアデコーダ１７から課金データチャージャ２５に対して、データ記録再生装置１０の複製／再生履歴情報（複製／再生ログ）が伝送される。複製ログには、複製したデータの識別子および／または複製の条件を含む。具体的には、複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報を含んでいる。

【０１２９】再生ログは、復号したディジタルデータの識別子および／または復号の条件を含む。具体的には、聴取した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報を含んでいる。この例では、再生時には、復号に対して課金される。

【０１３０】また、複製／再生ログには、ユーザ端末の所有者、ユーザデバイスとしてのデータ記録再生装置１０の識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコーダ１７と課金データチャージャ２５との間では、前述の図１に示した暗号処理部１１２と暗号処理および制御部２１を利用して、必要に応じて認証を行い、認証が成立すると、暗号化された複製／聴取権データおよび複製／再生ログの伝送がなされる。

【０１３１】複製／聴取権データは、決済センター２０３から通信路２０６例えば電話回線を介して課金データチャージャ２５に渡される。または、決済センター２０３から通信路２０７を介して販売端末２０５に渡された複製／聴取権データが通信路２０８を介して課金データチャージャ２５に渡される。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。

【０１３２】課金データチャージャ２５に吸い上げられた複製／再生ログは、通信路２０６を介して決済センター２０３に送られる。または、通信路２０８を介して販売端末２０５に渡される。販売端末２０５は、通信路２０７を介して決済センター２０３から聴取権データを受け取ると共に、再生ログを決済センター２０３へ送る。さらに、入手した聴取権データの代金を決済センター２０３に支払う。通信路２０７は、電話回線、インターネット等である。

【０１３３】決済センター２０３と聴取権データチャージャ２５との間では、通信路２０６を介して複製／聴取権データおよび複製／再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、認証と暗号化とがなされる。聴取権データの決済に関して、銀行、クレジットカード会社２０４が存在している。銀行、クレジットカード会社２０４は、予め登録してあるユーザの銀行口座から決済センター２０３の依頼に基づいて、課金データチャージャ２５に書き込んだ複製／聴取権データ相当する金額を引き落とす。

【０１３４】さらに、決済センター２０３は、レコード会社２０１から複製／聴取権データに関するサービスの管理の委託を受ける。また、決済センター２０３は、レコード会社２０１に対して複製／聴取権データに関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社２０１は、著作権管理機構２０２に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構２０２から著作権料を受け取る。

【０１３５】なお、通信路２０８の代わりに、ＩＣカードを利用することもできる。すなわち、課金データチャージャ２５および販売端末２０５は、ＩＣカードの書込み／読出し部を備えるようにする。そして、ＩＣカードを課金データチャージャ２５に差し込んだ時には、課金データチャージャ２５は、ＩＣカードに格納されている複製／聴取権データを吸い上げるとともに、複製／再生ログのデータをＩＣカードに書き込むようにする。ＩＣカードの複製／聴取権データは、課金データチャージャ２５に吸い上げられると、クリアされて零となる。

【０１３６】また、販売端末２０５にＩＣカードを差し込んだ時には、ユーザが必要な複製／聴取権データの度数を設定することにより、当該設定された複製／聴取権データがＩＣカードに書き込まれる。このとき、同時に、ＩＣカードに格納されていた複製／再生ログが販売端末２０５に吸い上げられ、ＩＣカードの複製／再生ログは、クリアされる。

【０１３７】以上説明したような課金システムにおいて、この実施の形態では、記録ルールまたは再生ルールとして、課金処理が必要な処理が設定されていた場合には、データ記録再生装置１０のセキュアデコーダ１７において、複製または再生についての課金処理が実行される。

【０１３８】図１１は、複製記録の際のステップＳ４８において、記録ルールが課金を伴なう記録と設定されている場合におけるステップＳ４９での処理のフローチャートである。

【０１３９】すなわち、先ず、セキュアデコーダ１７のメモリの複製権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップＳ８１）。課金処理が可能であると判別されたときには、記録（複製）を実行する（ステップＳ８２）。そして、記録が終了したことを確認すると（ステップＳ８３）、セキュアデコーダ１７のメモリの複製権データの度数を減じる（ステップＳ８４）。そして、複製ログとして、例えば複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報をそのメモリに記憶する（ステップＳ８５）。そして、課金処理を終了する。

【０１４０】一方、セキュアデコーダ１７のメモリの複製権データの度数の残が無く、課金処理が不可の場合には、複製権データの度数残が無い旨のメッセージを出し、ユーザに知らせる（ステップＳ８６）。そして、複製権データが追加されたか否か判別し（ステップＳ８７）、追加されたときには、ステップＳ８２に進み、記録を実行して、上述のステップＳ８３以降の処理を行なう。また、複製権データの追加が無かったときには、記録不可として（ステップＳ８８）、この課金処理ルーチンを終了する。

【０１４１】また、図１２は、再生の際のステップＳ７３において、再生ルールが課金を伴なう再生と設定されている場合におけるステップＳ７４での処理のフローチャートである。

【０１４２】すなわち、先ず、セキュアデコーダ１７のメモリの聴取権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップＳ９１）。課金処理が可能であると判別されたときには、再生データの暗号を解除する復号を実行する（ステップＳ９２）。そして、復号が完了したことを確認すると（ステップＳ９３）、セキュアデコーダ１７のメモリの聴取権データの度数を減じる（ステップＳ９４）。そして、再生ログとして、例えば再生した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報をそのメモリに記憶する（ステップＳ９５）。そして、課金処理を終了する。

【０１４３】一方、セキュアデコーダ１７のメモリの聴取権データの度数の残が無く、課金処理が不可の場合には、聴取権データの度数残が無い旨のメッセージを出し、ユーザに知らせる（ステップＳ９６）。そして、聴取権データが追加されたか否か判別し（ステップＳ９７）、追加されたときには、ステップＳ９２に進み、復号を実行して、上述のステップＳ９３以降の処理を行なう。また、聴取権データの追加が無かったときには、再生不可として（ステップＳ９８）、この課金処理ルーチンを終了する。

【０１４４】なお、ステップＳ９８では、完全に再生不可とするのではなく、さわりの部分やさびの部分のみの再生を可とするようにしてもよい。

【０１４５】［その他の実施の形態］上述の実施の形態においては、再生時には、ユーザＩＤモジュールは、データ記録再生装置あるいはパーソナルコンピュータには接続しなくても再生可能としたが、再生時にも、ユーザＩＤモジュールを接続しなければ、再生できないような仕組みとしてもよい。すなわち、不揮発性メモリ１４を設けずに、再生時にもユーザＩＤモジュールの接続を必須として、ユーザＩＤモジュールからのユーザＩＤと、再生データから検出したユーザＩＤとを照合するようにしても良い。

【０１４６】また、再生処理としては、上述の実施の形態と同様とするも、例えば、再生前に、データ記録再生装置に対するユーザＩＤモジュールの接続を確認し、不揮発性メモリ１４に記憶されているユーザＩＤと、使用者を示すユーザＩＤモジュールからのユーザＩＤとの照合を行って、使用者を確認してから、上述の再生動作を行うようにすることもできる。

【０１４７】また、上述の実施の形態の場合においては、記録時には、ユーザＩＤモジュールの認証確認は行うが、ユーザＩＤを用いた確認は行っていない。しかし、記録時に、ユーザＩＤモジュールをデータ記録再生装置に接続したときに、ユーザＩＤを用いたユーザＩＤモジュールの認証確認を行うようにしてもよい。

【０１４８】また、上述の実施の形態は、記録再生装置の場合であるが、記録専用装置や、再生専用装置にも、この発明は適用可能である。その場合、ユーザＩＤモジュールは、上述の第１および第２の実施の形態と同様の形態では、記録専用装置に付属すべきものである。再生専用装置の場合には、再生専用装置には、ユーザＩＤを、その不揮発性メモリに一旦登録すれば、再生時には、再生装置にユーザＩＤモジュールを接続しておく必要はない。

【０１４９】もっとも、これらの実施の形態にも、上述のその他の実施の形態を適用することも、勿論できる。

【０１５０】なお、上述の第１および第２の実施の形態におけるユーザＩＤ登録は、データ記録再生装置のうちの再生装置部分に対するユーザ登録である。前述の第１および第２の実施の形態では、記録装置に対しては、ユーザＩＤモジュールを必ず接続して、そのユーザＩＤを記録するようにするので、記録装置部分のみを考えた場合には、ユーザＩＤを登録する必要はない。

【０１５１】しかし、記録専用装置や記録再生装置の記録装置部分の機能を特定の使用者専用とする場合には、ユーザＩＤモジュールを用いて、ユーザＩＤを登録して不揮発性メモリに記憶しておき、記録の際にユーザＩＤが一致したときに、記録が可能となるようにする仕組みとすることもできる。

【０１５２】また、上述の実施の形態では、ユーザＩＤとしては、ユーザ名やモジュールＩＤを用いるようにしたが、使用者の指紋や声紋、あるいは脈などの各個人に固有の生体情報を使用するようにしても良い。その場合

に、再生装置では、不揮発性メモリに記憶されている生体情報のユーザＩＤと再生データから検出した生体情報のユーザＩＤとを照合するようにしても良いが、不揮発性メモリを設けずに、再生データから検出した生体情報のユーザＩＤと、指紋や声紋、あるいは脈などの生体情報入力手段から入力された生体情報のユーザＩＤとを照合するようにすることもできる。この場合に、生体情報入力手段は、ユーザＩＤモジュールを用いることができる。

【０１５３】なお、音楽会社などから提供される読み出し専用形式のディスクのように、市販される記録媒体は、「オリジナル」として扱うこととし、前述したように、所有者は無しとされる。ただし、この「オリジナル」から複製が行なわれた場合には、その複製には、前述したように、ユーザＩＤが記録され、所有者が特定されることになる。

【０１５４】また、上述の実施の形態では、ユーザ名については、特に制限を付けなかったが、ユーザ名は個人名であっても、ファミリー名のようなグループ名であっても良い。要するに、著作権法上「個人の使用の範囲内」と認められるような範囲で共有が可能である。

【０１５５】また、１台の記録ないし再生装置に、複数個のユーザＩＤを登録することができるようにして、前記１台の装置を、前記複数個のユーザＩＤに対応する複数の使用者で共有するようにすることもできる。

【０１５６】また、上述の実施の形態では、ユーザＩＤは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザＩＤを記録データに付加することができる。

【０１５７】また、上述の実施の形態では、記録時には、ユーザＩＤモジュール２０をデータ記録再生装置１０に接続することを必須としたが、記録時に、ユーザＩＤモジュール２０を接続することなく、データ記録再生装置１０の不揮発性メモリ１４に蓄えられているユーザＩＤ（特にモジュールＩＤ）と、記録対象のデータに付随するユーザＩＤとを比較照合するようにしてもよい。

【０１５８】また、記録ルールとして、不揮発性メモリ１４に記憶されているユーザＩＤと、記録対象のデータに付随するユーザＩＤとが一致したときには、ユーザＩＤモジュール２０はデータ記録再生装置１０には接続不要という設定を行なえるようにしてもよい。

【０１５９】また、記録対象のデータに付随するユーザＩＤというときには、記録対象のデータに埋め込まれていることのみを意味するのではなく、上述もしたように、記録媒体のＴＯＣエリアや、その他の記録対象データの記録部分とは別個のエリアから、ユーザＩＤを取得することも含む。また、インターネットからダウンロードしたデータを記録対象とする場合に、そのダウンロードデータの最初、中間あるいは最後に、ユーザＩＤが付加されるような場合も含む。

【０１６０】記録対象のデータは、データ記録再生装置１０において記録媒体から再生されたものではなく、アナログ入力とされた、あるいはデジタル入力とされたデータを含むものであることは言うまでもない。その場合に、その入力データは、ディスクから再生された再生データである必要もない。

【０１６１】なお、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

【０１６２】また、記録媒体としては、ディスクに限らず、カード形メモリや、半導体メモリ、ハードディスク装置のハードディスクなどであってもよい。さらに、記録対象となるデータは、前述もしたように、記録媒体から再生されたデータに限られるものではなく、有線電話回線や無線電話回線またはインターネットを通じて送られてくるデータであってもよい。

【０１６３】また、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

【０１６４】また、上述の実施の形態では、ユーザＩＤは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザＩＤを記録データに付加することができる。

【０１６５】

【発明の効果】以上説明したように、この発明によれば、記録時に、登録されたユーザＩＤを記録データと共に記録し、再生時には、不揮発性メモリ１４などに用意されるユーザＩＤと、記録媒体から読み出されたデータから検出されたユーザＩＤとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

【図面の簡単な説明】

【図１】この発明の第１の実施の形態を示すブロック図である。

【図２】この発明の第１の実施の形態の動作説明のためのフローチャートである。

【図３】この発明の第１の実施の形態の動作説明のためのフローチャートである。

【図４】この発明の第１の実施の形態の動作説明のためのフローチャートである。

【図５】この発明の第１の実施の形態における記録処理

の説明のためのフローチャートの一部である。

【図６】この発明の第１の実施の形態における記録処理の説明のためのフローチャートの一部である。

【図７】この発明の第１の実施の形態における再生処理の説明のためのフローチャートの一部である。

【図８】この発明の第１の実施の形態における再生処理の説明のためのフローチャートの一部である。

【図９】この発明の第２の実施の形態のブロック図である。

【図１０】この発明の実施の形態における課金処理システムの全体の概要を説明するための図である。

【図１１】この発明の実施の形態における記録時（複製時）の課金処理を説明するためのフローチャートである。

＊る。

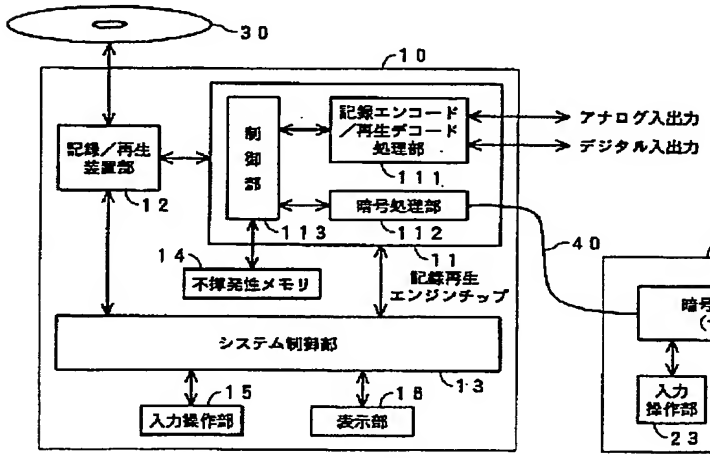
【図１２】この発明の実施の形態における再生時の課金処理を説明するためのフローチャートである。

【図１３】ＳＣＭＳ方式による複製世代制限方法を説明するための図である。

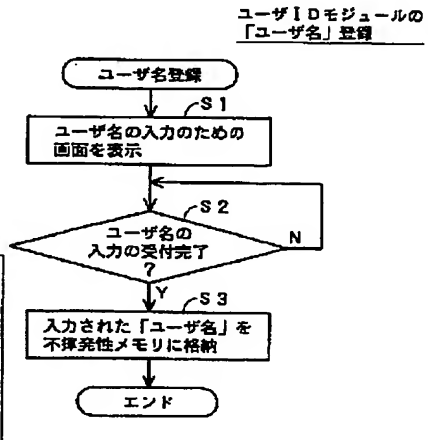
【符号の説明】

１０…データ記録再生装置、１１…記録再生エンジンチップ、１２…記録／再生装置部、１３…システム制御部、１４…不揮発性メモリ、１５…入力操作部、１６…表示部、２０…ユーザＩＤモジュール、２１…暗号処理および制御部、２２…不揮発性メモリ、２３…入力操作部、２４…表示部、３０…ディスク、４０…ケーブル、５０…パーソナルコンピュータ

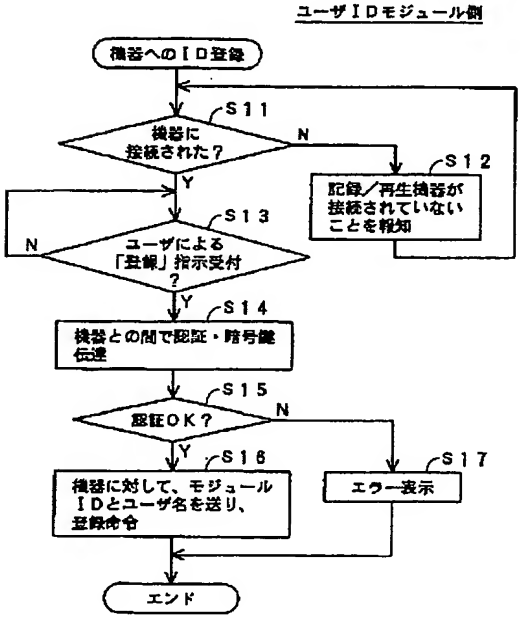
【図１】



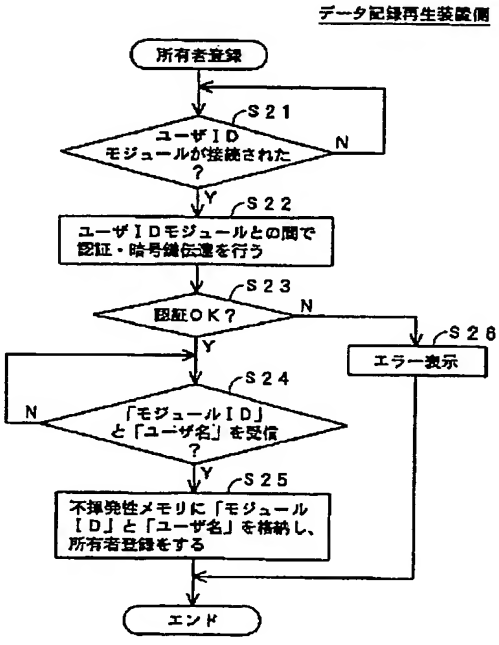
【図２】



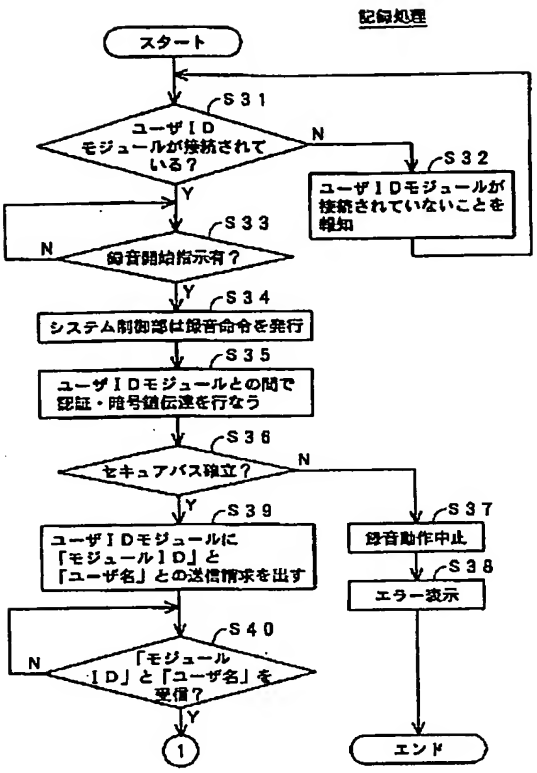
【図３】



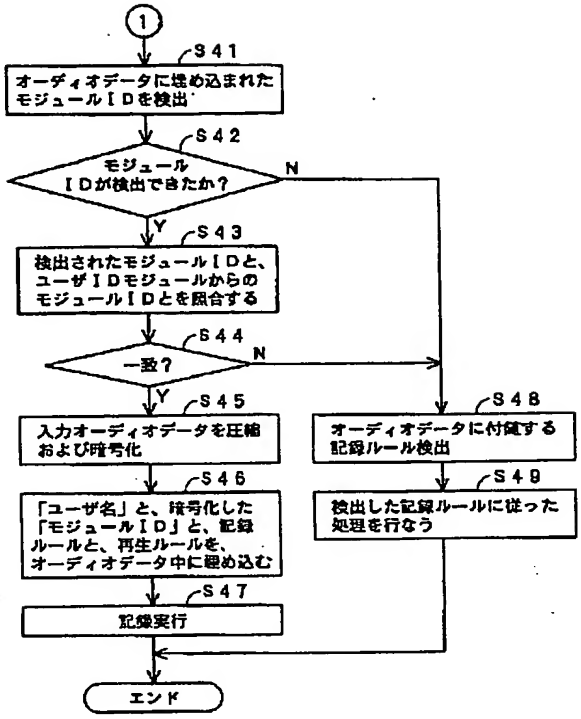
【図４】



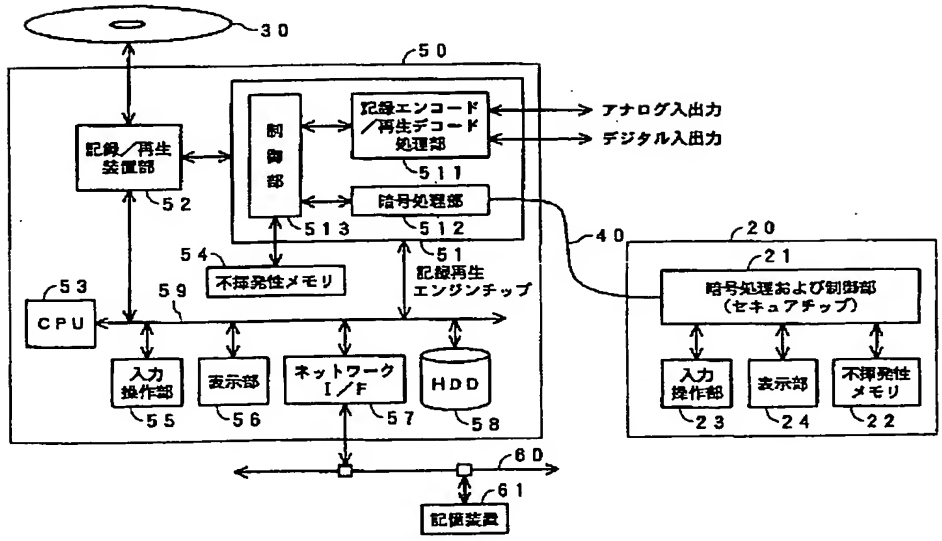
【図５】


記録処理
スタート
S31
ユーザＩＤ
モジュールが接続されて
いる？
N
S32
ユーザＩＤモジュールが
接続されていないことを
報知
Y
S33
N
録音開始指示有？
Y
S34
システム制御部は録音命令を発行
S35
ユーザＩＤモジュールとの間で
認証・暗号鍵伝達を行なう
S36
セキュアパス確立？
N
Y
S39
ユーザＩＤモジュールに
「モジュールＩＤ」と
「ユーザ名」との送信情求を出す
S37
録音動作中止
S38
エラー表示
S40
N
「モジュール
ＩＤ」と「ユーザ名」を
受信？
Y
1
エンド

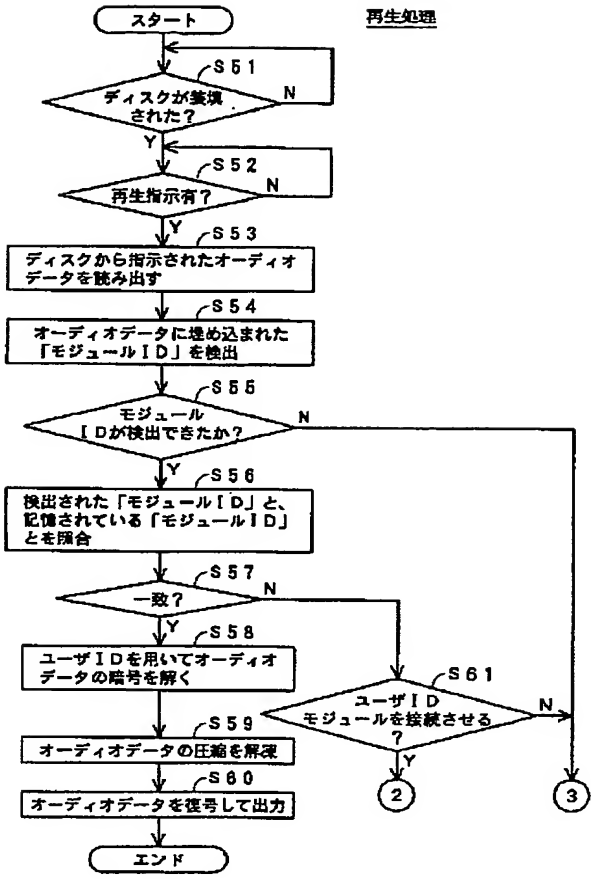
【図６】


1
S41
オーディオデータに埋め込まれた
モジュールＩＤを検出
S42
モジュール
ＩＤが検出できたか？
N
Y
S43
検出されたモジュールＩＤと、
ユーザＩＤモジュールからの
モジュールＩＤとを照合する
S44
一致？
N
Y
S45
入力オーディオデータを圧縮
および暗号化
S46
「ユーザ名」と、暗号化した
「モジュールＩＤ」と、記録
ルールと、再生ルールを、
オーディオデータ中に埋め込む
S47
記録実行
S48
オーディオデータに付随する
記録ルール検出
S49
検出した記録ルールに従った
処理を行なう
エンド

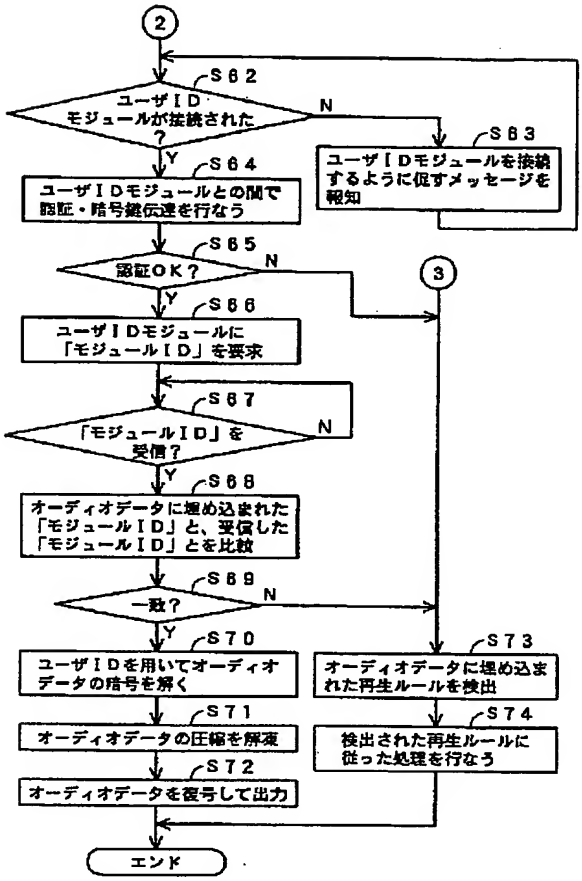
【図９】


30
50
記録／再生
装置部
52
制
御
部
記録エンコード
／再生デコード
処理部
511
暗号処理部
512
513
アナログ入出力
デジタル入出力
54
不揮発性メモリ
51
記録再生
エンジンチップ
53
CPU
59
入力
操作部
55
表示部
56
ネットワーク
I／F
57
HDD
58
60
61
記憶装置
40
20
21
暗号処理および制御部
（セキュアチップ）
入力
操作部
23
表示部
24
不揮発性
メモリ
22

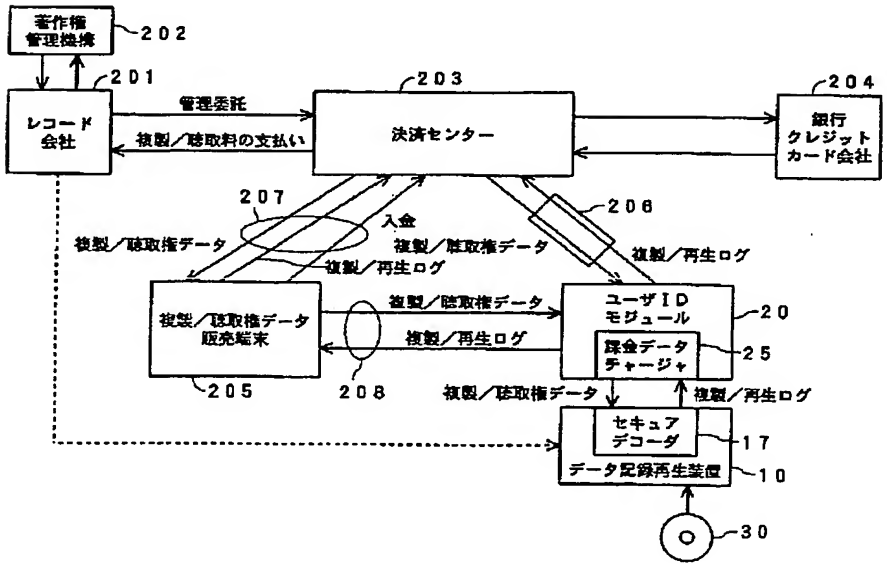
【図７】


再生処理
スタート
S51
ディスクが装填された？
N
Y
S52
再生指示有？
N
Y
S53
ディスクから指示されたオーディオデータを読み出す
S54
オーディオデータに埋め込まれた「モジュールＩＤ」を検出
S55
モジュールＩＤが検出できたか？
N
Y
S56
検出された「モジュールＩＤ」と、記憶されている「モジュールＩＤ」とを照合
S57
一致？
N
Y
S58
ユーザＩＤを用いてオーディオデータの暗号を解く
S59
オーディオデータの圧縮を解凍
S60
オーディオデータを復号して出力
エンド
S61
ユーザＩＤモジュールを接続させる？
N
Y
2
3

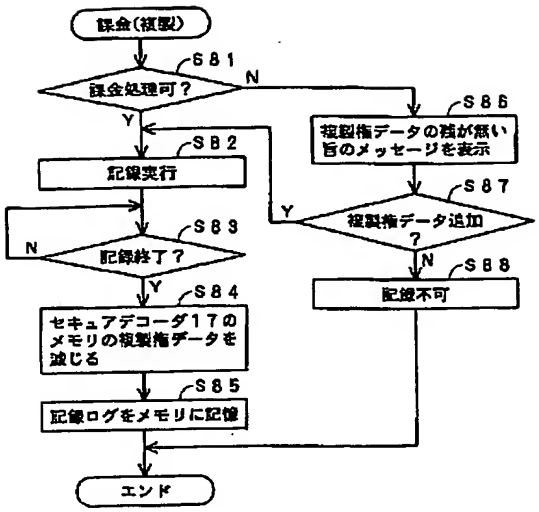
【図８】


2
S62
ユーザＩＤモジュールが接続された？
N
Y
S63
ユーザＩＤモジュールを接続するように促すメッセージを報知
S64
ユーザＩＤモジュールとの間で認証・暗号鍵伝達を行なう
S65
認証ＯＫ？
N
Y
3
S66
ユーザＩＤモジュールに「モジュールＩＤ」を要求
S67
「モジュールＩＤ」を受信？
N
Y
S68
オーディオデータに埋め込まれた「モジュールＩＤ」と、受信した「モジュールＩＤ」とを比較
S69
一致？
N
Y
S70
ユーザＩＤを用いてオーディオデータの暗号を解く
S71
オーディオデータの圧縮を解凍
S72
オーディオデータを復号して出力
S73
オーディオデータに埋め込まれた再生ルールを検出
S74
検出された再生ルールに従った処理を行なう
エンド

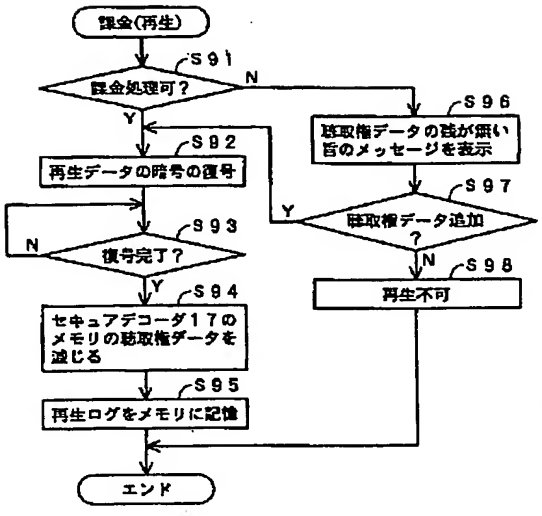
【図１０】


著作権管理機構
202
201
レコード会社
管理委託
複製／聴取料の支払い
203
決済センター
204
銀行クレジットカード会社
207
入金
複製／聴取権データ
複製／再生ログ
206
複製／聴取権データ
複製／再生ログ
複製／聴取権データ販売端末
205
208
複製／聴取権データ
複製／再生ログ
ユーザＩＤモジュール
20
課金データチャージャ
25
複製／聴取権データ
複製／再生ログ
セキュアデコーダ
17
データ記録再生装置
10
30

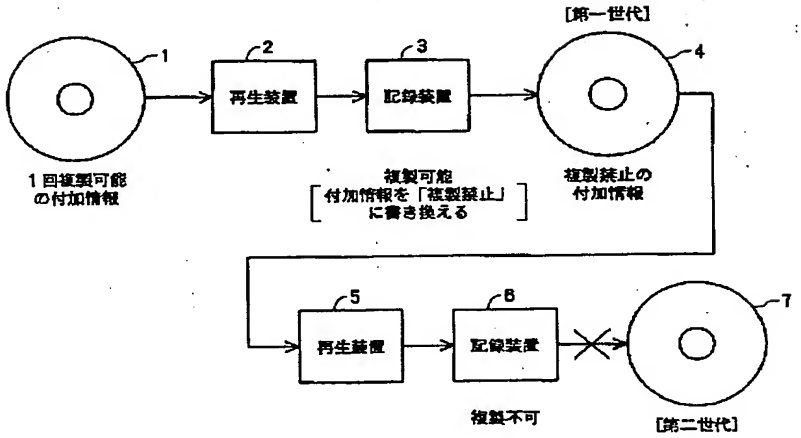
【図１１】



【図１２】



【図１３】



フロントページの続き

(72)発明者　鳥山　充
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5D044 AB02 AB05 AB07 BC05 BC06
CC06 DE50 DE54 EF05 FG18
GK12 GK17 HL02 HL08 HL11
5J104 AA07 AA13 AA14 EA04 EA26
KA01 KA15 KA16 KA17 KA18
MA01 NA01 NA02 NA27 NA36
NA37 NA39 NA41 PA11

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 302 944 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
16.04.2003 Bulletin 2003/16

(21) Application number: **01948047.4**

(22) Date of filing: **17.07.2001**

(51) Int Cl.[7]: **G11B 20/10**

(86) International application number:
PCT/JP01/06183

(87) International publication number:
WO 02/007161 (24.01.2002 Gazette 2002/04)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **17.07.2000 JP 2000216388**
30.08.2000 JP 2000260467

(71) Applicant: **Sony Corporation**
Tokyo 141-0001 (JP)

(72) Inventors:
- **INOKUCHI, Tatsuya, c/o SONY CORPORATION**
Tokyo 141-0001 (JP)
- **SAKO, Yoichiro, c/o SONY CORPORATION**
Tokyo 141-0001 (JP)
- **TORIYAMA, Mitsuru, c/o SONY CORPORATION**
Tokyo 141-0001 (JP)

(74) Representative: **Ayers, Martyn Lewis Stanley et al**
J.A. KEMP & CO.,
14 South Square,
Gray's Inn
London WC1R 5JJ (GB)

(54) METHOD AND APPARATUS FOR RECORDING AND/OR REPRODUCING DATA AND RECORD MEDIUM

(57) A method of recording and/or reproducing data to and/or from a recording medium is provided. A user identification data read from a recording medium having recorded therein main data to be recorded and/or reproduced and the user identification data is compared with a one read from a data recorder/player for recording or reproducing the main data, and the main data are recorded to or reproduced from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

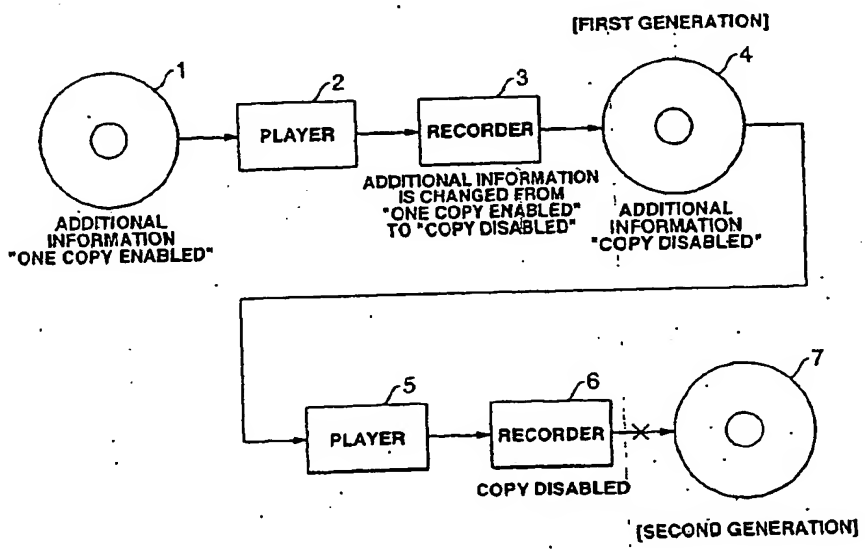


FIG.1

EP 1 302 944 A1

Description

Technical Field

[0001] The present invention relates to a method of and/or apparatus for recording and reproducing content data whose copyrights have to be managed, such as audio information, video information, game program and data, computer program, etc.

Background Art

[0002] As the digital contents have become prevalent, the infringement on their copyrights by illicit copying has given birth to a social problem. In analog recording to a tape medium, audio or video data are recorded in an analog manner and so copying of the data will result in a lower quality. In digital data recording or reproduction, however, a digital data recorder/player can be used to repeatedly copy audio or video data many times with no quality degradation, in principle.

[0003] Thus, the loss due to such illicit copying has become greater in the field of digital recording/reproduction than in the analog field, and thus it has become very important to prevent illicit copying with any digital recording/players.

[0004] To solve the above problem, it has been proposed to add copy-control information to digital contents and use the added information in order to prevent illicit copying of the digital contents.

[0005] For example, the copyright protection method employing a generation-limiting copy control called "SCMS (serial copy management system) is applied to digital data recorder/players for CD (compact disc), MD (mini disc; registered trademark), DAT (digital audio tape), etc. The SCMS copy-control method is to authorize to copy an audio content once but inhibit any further copying of the thus once copied audio content.

[0006] The SCMS copy-control method will be described in detail below with reference to FIG. 1.

[0007] For example, it is assumed here that a disc 1 has original-source audio signals digitally recorded therein. The digital audio signals are recorded in a predetermined recording format in the disc 1, and there is recorded in a specific area in the digital signals additional information indicating that the SCMS copy-control method permits to copy the digital audio signals only once.

[0008] A disc player 2 plays back the disc 1 to reproduce the digital audio signals from signals read from the disc 1, and sends the digital audio signals along with the additional copy-control information to a disc recorder 3. For sending the digital audio signals to the disc recorder 3, the disc player 2 will normally take a length of time equal to the time taken for reading the signals from the disc 1 (at the same speed).

[0009] Receiving the digital audio signals, the disc recorder 3 recognizes, when the information added to the audio signals indicates that the received digital audio signals may be copied only once, that the input digital signals can be copied. The disc recorder 3 will record the digital signals as a copy to another recordable disc 4. In this case, the disc recorder 3 rewrites the additional information from "one copy allowed" to "further copy inhibited". Thus, the digital signals as the copy and also the additional information "further copy inhibited" are recorded or copied to the disc 4.

[0010] In case the digital audio signals thus recorded as the copy in the disc 4 (first-generation disc) are read from the disc 4 played in another disc player 5 and supplied to another disc recorder 6, however, since the disc recorder 6 will detect that the additional information included in the digital signals is "further copy inhibited", the digital audio signals cannot further be recorded to any recordable disc 7.

[0011] In this case, the copying speed is equal to that at which the audio signals have been sent from the disc player 2. That is, if a standard playback time is taken for reproduction of the audio signals, the copying speed will be equal to a normal playback speed.

[0012] The "standard playback time" is a real-time playback speed for audio signals, namely, it is a playback speed at which audio signals can be perceived by the person having the ordinary ability of hearing. For example, the standard speed for reproduction of data depends upon each player and is independent of the human perception.

[0013] As above, the SCMS copy-control method protects the copyright of data by permitting a first-generation copying in a recorder while inhibiting a second-generation copying from the first-generation copy.

[0014] The SCMS method is intrinsically intended to prevent copyrighted data from being copied in a large amount for unauthorized commercial distribution, rather than to inhibit such a second-generation copying. Therefore, it is not negative against the currently prevailing copyright concept that "free copying within a range of private use".

[0015] Recently, a variety of recording/reproducing media such as an MD (mini disc; registered trademark) player, card-type memory player incorporating a semiconductor memory, etc. have been commercially available. Thus, users can selectively use the MD player, card-type memory player or the like as a playing medium as they currently like. In these circumstances, copying is frequently done by the use of any of the above players, and the SCMS copy-control method allowing to copy data only from an original medium will be inconvenient even for copying of the data only for private use.

[0016] Many of the recent personal computers are provided each with a CD playing function to store (copy) musical information distributed via a CD into a hard disc in a hard disc drive built in the personal computer and reproduce the musical information from the hard disc. Copying to the card-type memory player can be effected at such a high speed that copying from the hard disc in

the personal computer will be more convenient. More precisely, copying from the hard disc to the card-type memory player provides a second-generation copy while musical information stored in the hard disc cannot be copied to the card-type memory player.

Disclosure of the Invention

[0017] Accordingly, the present invention has an object to overcome the above-mentioned drawbacks of the prior art by providing a data recording method and apparatus not adopting the SCMS copy-control method but permitting free copying within the range of private use and effective prevention of illicit copying for unauthorized commercial distribution of data.

[0018] The above object can be attained by providing a method of recording and/or reproducing data to and/or from a recording medium, including steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for recording or reproduction of the main data to or from the recording medium; and
recording or reproducing the main data to or from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

[0019] Also the above object can be attained by providing a recording-medium recorder including:

a head to scan a recording medium having stored therein a user identification data along with main data;
a memory having a user identification data recorded therein; and
a controller to compare the user identification data read by the head from the recording medium with that read from the memory and control operations for reproduction of the main data from the recording medium on the basis of the result of comparison.

[0020] Also the above object can be attained by providing a recording-medium player, including:

a head to scan a recording medium having recorded therein encrypted data as well as at least a user identification data and reproduction management data;
a memory having a user identification data stored therein; and
a controller to compare the user identification data read by the head from the recording medium with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

[0021] Also the above object can be attained by providing a method of controlling data copying, including steps of:

comparing a user identification data read from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for copying of the main data; and
controlling data output when the user identification data extracted from the data in coincident with that read from the data recorder/player.

[0022] Also the above object can be attained by providing a data reproducing method including steps of:

comparing a user identification data extracted from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for reproduction of the main data; and
reproducing the data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

[0023] These objects and other objects, features and advantages of the present invention will become more apparent from the following detailed description of the best mode for carrying out the present invention when taken in conjunction with the accompanying drawings.

Brief Description of the Drawings

[0024]

FIG. 1 explains the SCMS-based copy-generating limiting method.
FIG. 2 is a block diagram of a first embodiment of the present invention.
FIG. 3 is a flow chart for explanation of the operations of the first embodiment of the present invention.
FIG. 4 is also a flow chart for explanation of the operations of the first embodiment of the present invention.
FIG. 5 is also a flow chart for explanation of the operations of the first embodiment of the present invention.
FIG. 6 is a flow chart for explanation of the recording operations made by the first embodiment of the present invention.
FIG. 7 is a flow chart for explanation of recording operations made by the first embodiment of the present invention.
FIG. 8 is a flow chart for explanation of playback operations made by the first embodiment of the present invention.
FIG. 9 is a flow chart for explanation of playback operations made by the first embodiment of the present invention.

FIG. 10 is a block diagram of a second embodiment of the present invention.

FIG. 11 is a flow chart for general description of the entire billing system in the embodiments of the present invention.

FIG. 12 is a flow chart for explanation of a billing made for recording (copying) in the embodiments of the present invention.

FIG. 13 is a flow chart for explanation of a billing made for playback in the embodiments of the present invention.

Best Mode for Carrying Out the Invention

[0025] The present invention will be described in detail concerning recording and reproduction of audio signals to and from a disc-shaped recording medium, by way of example.

[First embodiment]

[0026] FIG. 2 is a block diagram of the first embodiment of the data recording/playback system according to the present invention.

[0027] As shown in FIG. 2, the recording/playback system includes a data recorder/player 10 according to the present invention, and a user identification image server 20. The user identification data server 20 will also be referred to as "user ID module" in the following description. According to this embodiment, all the data recorder/players 10 are provided with terminals for connection of the user ID module 20. Information transferred between the data recorder/player 10 and user ID module 20 via the interconnection terminals is encrypted for security.

[0028] As shown, the data recorder/player 10 includes a recording/playback signal processor (will be referred to as "recording/playback engine chip" hereunder) 11, recording/playback unit 12, system controller 13, nonvolatile memory 14, input controller 15, and a display unit 16. The recording/playback engine chip 11 includes, as functional units, a recording encoder/playback decoder 111, encryption unit 112 to establish a communication bus for encrypted-data communication with the user ID module 20, and a controller 113.

[0029] The recording encoder/playback decoder 111 included in the recording/playback engine chip 11 is controlled by the system controller 13 to encode, for recording, analog or digital audio signals supplied thereto and provide the thus encoded signals to the recording/playback unit 12, for recording, as will be described later, and decode, for reproduction, the data reproduced from the recording/playback unit 12 and outputting the thus decoded signals, for data reproduction, as will also be described later.

[0030] The encryption unit 112 in the recording/playback engine chip 11 is connected to the user ID module 20 by a cable 40 in the embodiment shown in FIG. 2. In this embodiment, the encryption unit 112 functions, under the control of the system controller 13, to make mutual authentication with the user ID module 20 and establish a commumcation path to the user ID module 20 when they have successfully authenticated each other. In this case, to prevent any fraudulence such as a pretense as an authorized data recorder/player 10, a new encryption key for encryption and decryption is transmitted between the data recorder/player 10 and user ID module 20, and used to encrypt data to be transferred between the data recorder/player 10 and user ID module 20, before making any communication between the data recorder/player 10 and user ID module 20.

[0031] The controller 113 in the recording/playback engine chip 11 controls the recording encoder/playback decoder 111 and the encryption unit 112 according to a control signal supplied from the system controller 13, while controlling write and read of a user identification data to the nonvolatile memory 14 connected to the controller 113.

[0032] The recording/playback unit 12 is controlled by the system controller 13 to record the recorded signals from the recording/playback engine chip 11 to a disc 30, and also supplies the data read from the disc 30 to the recording/playback engine chip 11.

[0033] The system controller 13 provides a control conforming to an instruction given by the user operating the input controller 15, and sends necessary data to the display unit 16 for display on the screen of the latter. The display element of the display unit 16 may be a liquid crystal display, for example.

[0034] The user ID module 20 is accessory to one data recorder/player 10, and supplies a user identification data (will be referred to as "user ID" hereunder) to the data recorder/player 10. As shown in FIG. 2, the user ID module 20 includes an encryption/control unit (will be referred to as "security chip" hereunder) 21, nonvolatile memory 22, input controller 23 and a display unit 24.

[0035] The security unit 21 functions to make mutual authentication with the recording/playback engine chip 11 and establish a communication path to the recording/playback engine chip 11 when they have successfully authenticated each other. In this case, to prevent the aforementioned fraudulence such as a pretense, a new encryption key for encryption and decryption is transmitted between the data recorder/player 10 and user ID module 20 before making communication between the data recorder/player 10 and user ID module 20.

[0036] The nonvolatile memory 22 has module identification information unique to each user ID module 20 (will be referred to as "module ID" hereunder) such as a unique numeral value written therein at shipment from factory.

[0037] After purchasing the data recorder/player 10, the user shall operate the input controller 23 to register his or her name (user name) to the user ID module 20 accessory to his or her data recorder/player 10 while viewing the screen of the display unit 24.

[User name registration to user ID module 20]

[0038] FIG. 3 shows a flow of operations to be made for registering a "user name" to the user ID module 20.

[0039] First, the user ID module 20 displays a "user name" input screen on the display unit 24 to prompt the user to enter his name (user name) to the user ID module 20 (in step S1). When the user has entered his name by operating the input controller 23 while viewing the display on the display unit 24, the user ID module 20 will make sure that the user name has completely been entered via the input controller 23 (in step S2), and then store the thus entered "user name" into the nonvolatile memory 22. These operations are effected under the control of the security chip 21..

[0040] Note that when a registered user name check mode is selected via the input controller 23, the user name thus supplied and registered will be read from the nonvolatile memory 22 and displayed on the screen of the display unit 24, whereby the user can make sure the user name has been registered.

[0041] When the entered "user name" is correlated one-to-one with a "module ID" prestored in the nonvolatile memory 22, the module ID will substantially mean the user ID. That is to say, according to the present invention, the user ID means both the module ID and user name in one case, and only the module ID in another case.

[User ID registration to the data recorder/player]

[0042] After registering the user name to the user ID module 20, the user has to connect the user ID module 20 to the data recorder/player 10 for registration of his user ID to the data recorder/player 10.

[0043] FIGS. 4 and 5 show flows of operations effected in registering the user ID to the data recorder/player 10 by means of the user ID module 20. FIG. 4 shows a flow of operations made at the user ID module 20, while FIG. 5 shows a flow of operations made at the data recorder/player 10.

<Operations made at the user ID module 20>

[0044] As shown in FIG. 4, the user ID module 20 judges first whether it is connected to the data recorder/player 10 (in step S11). If the user ID module 20 judges in step S11 that it is not yet connected, it will inform the user, by displaying a list on the display unit 16 or otherwise, that the data recorder/player 10 is not yet connected to the user ID module 20, and prompt the user to connect the data recorder/player 10 to the user ID module 20 (in step S12).

[0045] When it is detected that the user ID module 20 is connected to the data recorder/player 10, the user ID module 20 waits for an "instruction for registration" given by the user via the input controller 23 (in step S13). When it is detected that the registration instruction has been accepted, the user ID module 20 will authenticate and validate the recording/playback engine chip 11 of the data recorder/player 10 and transmit an encryption key (in step S14).

[0046] The user ID module 20 judges whether it has successfully made the mutual authentication with the recording/playback engine chip 11 and established a communication path (in step S15). If the user ID module 20 has failed in the authentication and in establishment of the communication path, it will exit this routine of operation with display of an error message on the display unit 24 (in step S17). When the user ID module 20 has succeeded in establishment of the communication path in step S15, it will read the module ID and user name from the nonvolatile memory 22, encrypt them and send them along with a registration instruction to the data recorder/player 10 (in step S16).

<Operations made at the data recorder/player 10>

[0047] As shown in FIG. 5, the data recorder/player 10 first waits until the user ID module 20 is connected thereto. When it judges that the user ID module 20 is connected (in step S21), the recording/playback engine chip 11 will authenticate and validate the user ID module 20 and transmit an encryption key (in step S22).

[0048] The recording/playback engine chip 11 judges whether it has successfully authenticated the user ID module 20 and established a communication path could (in step S23). If it is judged in step S23 that the data recorder/player 10 has failed in the authentication and in establishment of the communication path, it will exit this routine of operation with display of an error message on the display unit 16 (in step S26).

[0049] When the recording/playback engine chip 11 judges in step S23 that the communication could be established, it will wait for a registration instruction including "module ID" and "user name" sent from the user ID module 20 (in step S24). Upon confirmation of that reception, the recording/playback engine chip 11 will store the received module ID and user name into the nonvolatile memory 14 to register the device owner (in step S25).

[0050] Note that when a registered user name check mode is selected via the input controller 15, the user name thus supplied and registered will be read from the nonvolatile memory 14 and displayed on the screen of the display unit 16, whereby the user can make sure that the user name has been registered.

[0051] The user ID of the data recorder/player 10, thus registered once, can be re-set to another user ID by re-registering using the user ID module 20.

[Recording operations made at the data recording/player 10].

[0052] Next, operations made at the data recorder/player 10 for recording data will be described with ref-

erence to the flow charts shown in FIGS. 6 and 7.

[0053] For data recording in this embodiment, the user ID module 20 has to be connected to the data recorder/player 10. That is, the data recorder/player 10 first judges whether the user ID module 20 is connected thereto (in step S31). If it judges in step S31 that the user ID module 20 is not yet connected thereto, it will inform the user, by displaying on the display unit 16, that the user ID module 20 is not connected, and prompt to connect the user ID module 20 to the data recorder/player 10 (in step S32). In this case, the prompt to the user may be a video message or voice message like "the user ID module is not yet connected. For recording, connect the user ID module". The video message is displayed on the display unit 16.

[0054] If the data recorder/player 10 detects in step S31 that the user ID module 20 is connected thereto, it will wait for an "instruction for recording" given by the user via the input controller 15 (in step S33). When it is detected in step S33 that a "recording instruction" is received, the system controller 13 of the data recorder/player 10 supplies a recording instruction to the recording/playback engine chip 11 and recording/playback unit 12 to make preparations for data recording (in step S34).

[0055] Next, the recording/playback engine chip 11 authenticates and validates the security chip 21 in the user ID module 20, and transmits an encryption key (in step S35). The recording/playback engine chip 11 judges whether it has successfully authenticated the security chip 21 and established a communication path (in step S36). If it judges in step S36 that it has failed in the authentication of the security chip 21 and thus in establishment of a communication path, the recording/playback engine chip 11 will cease the recording procedure (in step S37) and then exit this routine of operation with display of an error message on the display unit 24 (in step S38).

[0056] When the recording/playback engine chip 11 judges in step S36 that the communication path could be established, it will issue a request for sending a user ID, that is, a module ID and user name in this case, to the user ID module 20 (in step S39).

[0057] In response to the request for sending the user ID, the security chip 21 in the user ID module 20 reads the module ID and user ID from the nonvolatile memory 22, encrypts them and sends them to the data recorder/player 10. The recording/playback engine chip 11 in the data recorder/player 10 will check if the module ID and user ID have been received by the data recorder/player 10 (in step S40).

[0058] After making sure the reception of the module ID and user ID in step S40, the recording/playback engine chip 11 tries to detect the module ID buried in audio data (in step S41), and judges whether the module ID could be detected (in step S42). If the module ID could be detected in step S42, the recording/playback engine chip 11 collates, by comparison, the detected module ID with a one available from the user ID module 20 (in step S43).

[0059] The recording/playback engine chip 11 judges whether the collation made in step S43 shows that both the module IDs is coincident with each other (in step S44). When both the module IDs are found to be is coincident with each other, the recording/playback engine chip 11 enables the recording, compresses the input audio data and encrypts them with the received user ID being taken as an encryption key (in step S45).

[0060] In this case, however, only the user name, only the module ID or both may be used as the encryption key.

[0061] There will be buried in the audio data compressed and encrypted in step S45 "user name" and "module ID" available from the user ID module 20 (in step S46). In this case, the module ID is encrypted before being buried to improve the concealment of the user ID. Further in step S46, a recording rule and reproduction rule are buried in the audio data to be recorded.

[0062] As above, the audio data in which the encrypted user ID etc. are buried are recorded to the disc 30 as a recording medium (in step S47).

[0063] On the other hand, if the module ID could not be detected in step S42 and when there is found in step S44 no coincidence between the module ID detected from the audio data and module ID available from the user ID module 20, the recording rule buried in the audio data is detected (in step S48) and operations conforming to the detected recording rule are effected (in step S49).

[0064] For burying information such as the recording rule, a technique called "digital watermarking" or any other well-known burying technique may be used. Also, such information may be buried not in audio data but in a recording area other than a recording area in which audio data are recorded such as an area where TOC (table of contents) data is recorded or in a sub code area.

[0065] The above-mentioned recording rules to be buried include the following of which any one is selected from them for burying in audio data:

R1 Recording (copying) is allowed for free
R2 Recording (copying) is allowed at cost
R3 Free recording (copying)
R4 Recording (copying) is inhibited

Contents of the recording rule themselves may be recorded as information about the recording rule or there may also be recorded information indicating which one of the above-mentioned rules R1 to R4 is to be buried.

[0066] The rule R1 "recording (copying) is allowed for free" permits to record audio data only with a user ID buried in audio data. In this embodiment, this rule is followed to record audio data to a recording medium, such as a read-only disc (will be referred to as "ROM type" disc hereunder) made by a recording company using an authoring apparatus, without any user ID being buried

since the disc is not yet owned by anybody at this stage. So, this rule is applied when recording (copying) audio data from a ROM-type recording medium.

[0067] The above rule R2 "recording (copying) is allowed at cost" permits a recorder capable of billing to record audio data only when the billing has been made. Under this rule, a recorder not capable of the billing is inhibited from recording audio data. The billing will be described in detail later using an example.

[0068] The rule R3 "free recording (copying)" permits to record (copy) audio data with no user ID being buried in the audio data. Further, the rule R4 "recording (copying) is inhibited" permits no recording of any audio data.

[0069] As above, the recording rules are applied when there is no coincidence between user IDs as well as when no user ID can be detected from audio data to be recorded. However, one recording rule may be recorded for application when no coincidence is detected between the user IDs while another recording rule may be recorded for application when no valid user ID can be detected.

[0070] For reproducing audio data in this embodiment, a user ID buried in the audio data is collated with a one stored in the nonvolatile memory 14 as will be described in detail later. When both the IDs are found to be coincident with each other, the audio data can be reproduced. In this embodiment, when no user ID can be detected in the audio data to be reproduced or when the result of collation is that the user IDs show no coincidence between them, a reproduction rule (playback condition) specifying how the audio data are to be processed is buried in the audio data in step S46.

[0071] Information about the reproduction rule may be buried in audio data using the digital watermarking or any other well-known burying technique as in the case of the aforementioned recording rule. Also, such information may be buried not in audio data but in a recording area other than a recording area in which audio data are recorded such as an area where TOC (table of contents) data is recorded or in a sub code area.

[0072] When there is no coincidence between user IDs, any one is selected from the following for burying in the audio data:

PB1 Reproduction is allowed for free
PB2 Reproduction is inhibited (reproduction is disabled)
PB3 Reproduction is allowed at cost
PB4 Reproduction is limitatively allowed

Contents of the reproduction rule themselves may be recorded as information about the reproduction rule or there may also be recorded information indicating which one of the above-mentioned rules PB1 to PB4 is to be buried.

[0073] The rule PB1 "reproduction is allowed for free" permits to always reproduce audio data independently of any user ID registered in the player. The rule PB2 "reproduction is inhibited (reproduction is disabled)" inhibits audio data from being reproduced when there is no coincidence between the user ID buried in the audio data and the user ID registered in the player. In this embodiment, since audio data are recorded, with no user ID buried therein, to a recording medium such as a ROM-type disc made by a recording company by the authoring apparatus as above, the rule PB1 is recorded in the audio data for application when no valid user ID can be available from the reproduced audio data.

[0074] Also, the rule PB3 "reproduction is allowed at cost" permits a player capable of billing to reproduce audio data when the billing is possible. If the player is not capable of such billing, audio data cannot be reproduced. Note that the billing will be described in detail later taking an example.

[0075] The rule PB4 "reproduction is limitatively allowed" permits to reproduce audio data for test-listening to all or a part of the audio data. After completion of the test-listening mode, the rule PB2 or PB3 is applied to the reproduction of audio data. For the test-listening, any of the following is allowed:

(a) Free reproduction by n times, for example, once
(b) Free reproduction for m seconds
(c) Free reproduction of most affecting passage or climax part

[0076] When the test-listening mode (a) or (b) is applied for the reproduction rule PB4 "reproduction is limitatively allowed", information about the test-listening history of audio data identified with an ID content (identification code) such as ISRC (International Standard Recording Code), for example, number of times of test-listening, seconds for which the test-listening has been made, etc., is registered in the player correspondingly to the ID content.

[0077] In this embodiment, the reproduction rule is applied in common when no coincidence is found between the user IDs for data reproduction as well as when no valid user ID is available from reproduced audio data. However, one reproduction rule may be recorded for application when no coincidence is found between user IDs while another reproduction rule may be recorded for application when no valid user ID is available from audio data.

[0078] For example, in case a recording medium such as a ROM-type disc or the like made by a recording company using an authoring apparatus has recorded therein a specific ID like "ORIGINAL" indicating that the recording medium is an original, the player, having detected the specific ID, should be allowed to reproduce audio data from the recording medium even if the specific ID is not coincident with the user ID of the player itself. Therefore, in case a reproduction rule is to be buried in audio data, it should be "reproduction is allowed".

[0079] On the other hand, in case it is prescribed that

such a specific ID should be recorded, by burying or otherwise, in audio data recorded in a recording medium such as a ROM-type disc or the like, the audio data may be taken as illicitly recorded data if no valid user ID is available in the player. Therefore, the reproduction rule should be "reproduction is inhibited" in this case.

[0080] One of the above reproduction rules can be used in common in recording media such as ROM-type discs made by recording companies using an authoring apparatus in case it is prescribed that no user data should be recorded in the recording media.

[Reproducing operations made at the data recorder/player 10]

[0081] Next, operations made at the data recorder/player 10 for reproducing audio data having been recorded as above will be described with reference to FIGS. 8 and 9.

[0082] First, a recorded disc is loaded into the data recorder/player 10. Recognizing when the recorded disc is set in the data recorder/player 10 (in step S51), the recording/playback engine chip 11 will wait for a playback instruction from the user. When the recording/playback engine chip 11 has recognized the playback instruction given by the user via the input controller 15 (in step S52), it reads audio data which it has thus been instructed to reproduce from the disc (in step S53).

[0083] A user ID buried in the thus read audio data is detected. In this embodiment, an encrypted module ID of the user ID is decrypted to detect the user ID (in step S54). It is judged whether the module ID could be detected (in step S55). If the module ID could not be detected, a reproduction rule buried in the audio data to be reproduced is detected (in step S73) and a due step is taken according to the detected reproduction rule (in step S74).

[0084] When it is judged in step S55 that the module ID could be detected, the detected module ID is collated, by comparison, with a one stored in the nonvolatile memory 14 (in step S56).

[0085] It is judged whether the module IDs are coincident with each other (in step S57). If it is judged in step S57 that the module IDs are coincident with each other, the encrypted audio data for which the user ID is used are decrypted (in step S58), and decompressed, that is, expanded (in step S59). The expanded or decompressed audio data are decoded before being outputted (in step S60).

[0086] On the other hand, if it is judged in step S57 that there is no coincidence between the module ID detected from the audio data read from the disc 30 and that read from the nonvolatile memory 14, it is judged whether the data recorder/player 10 has been set to have the user connect the user ID module 20. If the result of judgment is that no such setting has been made, the reproduction rule buried in the audio data to be reproduced is detected (in step S73) and a due step is taken according to the detected reproduction rule (in step S74). In this embodiment, playback of the disc 30 is inhibited, for example.

[0087] The above playback inhibition includes also blocking of the data recorder/player 10 from providing normal output of reproduced audio data. Namely, the data recorder/player 10 outputs a noise as the playback output. Alternately, the data recorder/player 10 may be adapted to provide a message like "this is a playback of an illicitly copied recording medium" instead of the playback output.

[0088] If it is judged in step S61 that the data recorder/player 10 has been set to have the user connect the user ID module 20, the data recorder/player 10 will judge whether the user ID module 20 is connected (in step S62). If it is judged in step S62 that the user ID module 20 is not connected, the data recorder/player 10 will inform the user of the fact and prompt the user to connect the user ID module 20 (in step S63).

[0089] When it is detected that the user ID module 20 is connected to the data recorder/player 10, the recording/playback engine chip 11 makes mutual authentication and validation with the user ID module 20 and transmits an encryption key (in step S64). Further the recording/playback engine chip 11 judges whether the mutual authentication and communication path establishment have successfully been made between the recording/playback engine chip 11 and user ID module 20 (in step S65). If the mutual authentication could not be made and the communication path could not be established between the recording/playback engine chip 11 and user ID module 20, the recording/playback engine chip 11 takes a due step according to the reproduction rule buried in the audio data (in steps S73 and S74). In this embodiment, playback of the disc 30 is inhibited as above.

[0090] When it is judged in step S65 that the communication path could be established between the recording/playback engine chip 11 and user ID module 20, the recording/playback engine chip 11 will send, to the user ID module 20, a request for sending a module ID in the user ID, in this embodiment (in step S66).

[0091] In response to the sending request from the recorder/playback engine chip 11, the security chip 21 in the user ID module 20 reads a module ID from the nonvolatile memory 22, encrypts it and sends the encrypted module ID to the data recorder/player 10. When the recording/playback engine chip 11 in the data recorder/player 10 validates the module ID sent from the user ID module 20 (in step S67), it will collate, by comparison, the module ID detected from the data read from the disc 30, with that received and decrypted or decoded (in step S68).

[0092] The recording/playback engine chip 11 judges whether the module IDs are coincident with each other (in step S69). When there is no coincidence between the module IDs, the recording/playback engine chip 11 will take a due step according to the reproduction rule buried in the audio data (in steps S73 and S74). As

above, playback of the disc 30 is inhibited in this embodiment.

[0093] When the module IDs are coincident with each other, the encrypted audio data are decrypted or decoded with the user ID (in step S70), decompressed or expanded (in step S71). The decompressed or expanded audio data are decoded and outputted (in step S72).

[0094] In this embodiment, data are recorded to a disc 30 with a registered user ID buried in the data, and a user ID registered in the nonvolatile memory 14 and a user ID detected from the data read from the disc 30 are compared with each other, as having been described above. When the result of comparison shows that the user IDs are coincident with each other, the data read from the disc 30 are normally reproduced and outputted. Thus, audio data can only be copied for private use.

[0095] Also in this embodiment, since the user ID module 20 is adapted to record data only when it is connected to the data recorder/player 10, audio data can only be copied for private use.

[0096] In this embodiment, the recording side is limited as above while at the playback side, a user ID registered in the nonvolatile memory 14 is compared with a user ID detected in the data read from the disc 30 to judge whether the user IDs are coincident with each other, and so for data recording, the user ID module 20 may not be connected to the data recorder/player 10. Namely, the user can reproduce the data with a greater convenience.

[0097] For "free copying only forprivate use", information about a personally acquired right of listening (information about all contents which it has been authorized to reproduce for private listening) may be recorded to a personal IC card which has to be inserted into the player, for reproducing the contents. This is just an example. In this case, to prevent the IC card from being used by any other user, the users are managed for each to have an exclusive IC card.

[0098] Since the IC card has recorded therein each user's right of listening for all the contents, the user can freely copy the contents. In this case, however, the user has to carry on the IC card which is to be inserted into the player each time he is going to copy the contents for listening, which will be a great inconvenience.

[0099] That is, the above embodiment is very convenient since it eliminates the above inconvenience since it requires such an IC card.

[0100] In this embodiment, since data are encrypted, for recording, with a user ID buried as an encryption key in the data, the recorded data can only be decrypted and decoded for reproduction when the user IDs are coincident with each other, which surely allows the data to be reproduced solely within a range of private use.

[0101] Note that use of a user ID not as an encryption key but as information about encryption such as information intended for acquisition of a key for encryption of data to be recorded is expectable to provide a similar effect. However, in case the recording or reproduction rule allows data recording or reproduction even when there is no coincidence between user IDs, the user ID may not always be used as the encryption key.

[0102] In the above embodiment, information about a user ID from the user ID module 20 is encrypted and sent to the data recorder/player 10, so that the user ID can effectively be concealed.

[0103] In this embodiment, since recording and reproduction rules are buried in audio data, information about these rules is detected from the audio data. In case information about recording and reproduction rules is recorded in TOC data or TOC area, however, the information should be acquired before recording or reproducing audio data.

[0104] In case audio data have been compressed and blocked, recording and reproduction rules may be buried in a space between blocks. In this case, information about the recording and reproduction rules can be extracted for decompression and decoding of the audio data.

[0105] In case the data recorder/player 10 is designed to accommodate a plurality of recording media together for simultaneous reproduction and recording and also for data recording (copying), information about recording and reproduction rules may be acquired from TOC data or reproduced data in a disc at the reproducing side in advance.

[0106] In the aforementioned embodiment of the present invention, recording and reproduction rules have to be recorded in audio data. Note however that by designing the system so that one of the above recording and reproduction rules is always applied when no user ID is available or when there is no coincidence between user IDs, it becomes unnecessary to record the recording and reproduction rules in the audio data.

[Second embodiment]

[0107] In the second embodiment of the present invention, the data recorder/player is installed in a personal computer. FIG. 10 is a block diagram of a system to which the second embodiment is applied.

[0108] As shown, the system according to the second embodiment includes a personal computer 50 and the user ID module 20 used in the aforementioned first embodiment.

[0109] The personal computer 50 has terminals for connection of the user ID module 20. Information transferred between the personal computer 50 and user ID module 20 via the terminals for connection of the user ID module 20 is all encrypted.

[0110] Similarly to the data recorder/player 10 according to the first embodiment, the personal computer 50 includes a recording/playback engine chip 51, recording/playback unit 52 and a nonvolatile memory 54, and has connected thereto a CPU 53, input controller 55, display unit 56, network interface 57 and a hard disc drive 58 via a system bus 59. The system bus 59 has

also connected thereto the recording/playback engine chip 51 and recording/playback unit 52.

[0111] The network interface 57 is connected to a memory 61 connected to a network 60. The network 60 may be a local area network (LAN) or Internet. In case the network 60 is the Internet, the memory 61 will be a recorder provided in a predetermined server or the like.

[0112] In this second embodiment, a user name is supplied for registration to the user ID module 20 as in the aforementioned first embodiment, and further the user ID is registered from the user ID module 20 into the personal computer 50. Thus, the user ID is registered into the nonvolatile memory 54.

[0113] The second embodiment uses, as the recording medium, not only the disc 30 as in the first embodiment but the memory 61 connected to the hard disc drive 58 and network 60.

[0114] In data recording in the second embodiment, the data will flow between an input source and recording medium in combination as follows:

(1) Analog or digital input to disc 30
(2) Analog or digital input to hard disc drive 58
(3) Analog or digital input to memory 61
(4) Disc 30 to hard disc drive 58
(5) Disc 30 to memory 61
(6) Hard disc drive 58 to disc 30
(7) Hard disc drive 58 to memory 61
(8) Memory 61 to disc 30
(9) Memory 61 to hard disc drive 58

[0115] In addition to the above nine combinations, data transfer from one memory to another in the network 60 may be considered as one of the recording operations. In each of the recording operations in the second embodiment, the user ID module 20 has to be connected to the personal computer 50 as in the first embodiment and a user name and module ID acquired from the user ID module 20 are buried in audio data. In this case, the module ID is to be encrypted as in the first embodiment.

[0116] For data recording to the hard disc drive 58 in this case, data encoded in the recording/playback engine chip 51 are sent to the hard disc drive 58 via the system bus 59, not via the recording/playback unit 52, and thus stored into the hard disc drive 58.

[0117] For data recording to the memory 61, data encoded in the recording/playback engine chip 51 are sent over the network 60 to the memory 61 via the system bus 59 and network interface 57, not via the recording/playback unit 52, and thus stored into the memory 61.

[0118] For reproduction of audio data from any of the disc 30, hard disc drive 58 and memory 62, a user ID detected in reproduced data is collated with a one stored in the nonvolatile memory 54 as in the aforementioned first embodiment. When they are coincident with each other, it is allowed to reproduce and output the audio data.

[0119] The second embodiment is as effective as the aforementioned first embodiment, and can allow a quick copying of audio data by the hard disc drive 58 solely for a private use by the user. The data transfer to the memory via the network can be considered as one manner of recording (copying) and is allowed only for the private use by the user.

[Example of billing operations]

[0120] Next, an embodiment of the present invention in which billing-based recording and reproduction rules are applied will be described with reference to FIG. 11 showing an example of billing system in which distribution and transfer of musical contents are omitted. The data recorder/player 10 included in this embodiment is adapted to record data for copying. That is, with the data recorder/player 10, data from a disc can be recorded to another disc.

[0121] For billing in this embodiment, right-of-copying data is used for recording, while right-of-listening data is used for playback. These right-of-copying and right-of-listening data are stored in an IC card or in a security decoder 17 provided in the data recorder/player 10.

[0122] The right-of-copying data and right-of-listening data are a number of times data can be copied and a number of times data can be reproduced, respectively, for example. Each time the data recorder/player 10 records or reproduces data for which the user is billed, each of the numbers is decremented.

[0123] The right-of-copying and right-of-listening data can be rewritten by a user's own right-of-copying/-listening data charger or a right-of-copying/-listening data selling terminal 205 placed at a shop under the management by a right-of-copying/listening data management company. In this embodiment, the right-of-copying/listening data charger is provided as a billing data charger 25 in the user ID module 20.

[0124] Between the security decoder 17 of the data recorder/player 10 and the right-of-copying/-listening data selling terminal 205 placed in a settlement center 203, records shop, convenience store or the like, there is provided the billing data charger 25 which functions as a right-of-listening data relay.

[0125] The settlement center 203 is provided for settlement in relation with a recording company 201, copyright management organization 202 and data recorder/player 10 as a user device. The settlement center 203 includes an authentication/billing server, and makes a settlement in relation with a bank or credit card company 204.

[0126] In FIG. 11, a broken line indicates the distribution from the recording company 201 of a recording medium (optical disc, memory card or the like) having musical contents recorded therein and which is to be played in the data recorder/player 10. The distribution of musical contents may be done in any other different suitable manners. The data recorder/player 10 can record the

musical contents to a recording medium (optical disc, memory card or the like) 30.

[0127] In this embodiment, the security decoder 17 in the data recorder/player 10 and billing data charger 25 in the user ID module 20 communicate with each other via a cable communication path to transfer right-of-copying/-listening data from the billing data charger 25 to a memory in the security decoder 17. The right-of-copying/listening data corresponds to a permitted number of times of recording (copying) or a permitted time length of recording (copying)/permitted number of times of reproduction or to a permitted time length of reproduction in the data recorder/player 10.

[0128] The security decoder 17 of the data recorder/player 10 sends copying/reproduction log of the data recorder/player 10 to the billing data charger 25. The copying log includes identifiers for copied data and/or copying conditions. More particularly, it includes information such as identifiers for copied contents, types of the contents, number of times of copying, copying time, etc.

[0129] The reproduction log includes identifiers for decoded digital data and/or decoding conditions. More particularly, it includes information such as identifiers for musical contents to which the user has listened, types of the contents, number of times of reproduction, reproducing time, etc. In this embodiment, billing is made to decoding for data reproduction.

[0130] The copying/reproduction log also includes identifiers to identify a billing object such as owner of the user terminal, identifier for the data recorder/player 10 as a user device, etc. Between the security decoder 17 and billing data charger 25, there is made authentication by the encryption unit 112 and encryption/control unit 21 shown in FIG. 2 when necessary. When the authentication could be made between the encryption unit 112 and encryption/control unit 21, encrypted right-of-copying/listening data and copying/reproduction log are transmitted.

[0131] The right-of-copying/-listening data are delivered from the settlement center 203 via a communication path 206, for example, a telephone line, to the billing data charger 25. Alternatively, right-of-copying/-listening data delivered from the settlement center 203 to the right-of-copying/-listening data selling terminal 205 via a communication path 207 are delivered to the billing data charger 25 via a communication path 208. Also in this case, authentication and encryption are effected between the settlement center 203 and billing data charger 25 for example to assure the security.

[0132] The copying/reproduction log sent to the billing data charger 25 is sent to the settlement center 203 via the communication path 206. Alternatively, the copying/reproduction log is delivered to the right-of-copying/-listening data selling terminal 205 via the communication path 208. The right-of-copying/-listening data 205 receives the right-of listening data from the settlement center 203 via the communication path 207 while sending the reproduction log to the settlement center 203. Further, the right-of-copying/-listening data selling terminal 205 will pay the charge for the thus acquired right-of-listening data to the settlement center 203. The communication path 207 may be a telephone line, Internet or the like.

[0133] Between the settlement center 203 and billing data charger 25, there is transferred the right-of-copying/-listening data and copying/reproduction log via the communication path 206. Also in this case, authentication and encryption for data transfer are effected between the settlement center 203 and billing data charger 25 to assure the security. The bank and credit card company 204 are included in the system for the purpose of paying the charges for the right-of-listening data. The bank or credit card company 204 will debit a money equivalent to the right-of-copying/-listening data written to the billing data charger 25 against a pre-registered user's account upon request from the settlement center 203.

[0134] Further, the settlement center 203 is entrusted by the recording company 201 to manage the servicing of the right-of-copying/-listening data. The settlement center 203 provides right-of-copying/-listening data-related techniques to the recording company 201, and also pays for the listening to the musical data. The recording company 201 registers its copyrights in the copyright management organization 202 to request the latter for management of the copyrights and receive corresponding royalties from the copyright management organization 202.

[0135] Note that an IC card may be used instead of the communication path 208. More particularly, the billing data charger 25 and right-of-copying/-listening data selling terminal 205 are provided each with an IC card writer/reader. When the IC card is inserted into the billing data charger 25, the latter will acquire the right-of-copying/listening data from the IC card and write the copying/reproduction log data to the IC card. When the right-of-copying/-listening data in the IC card is taken up by the billing data charger 25, it will be cleared to zero.

[0136] When a necessary number of times in the right-of-copying/-listening data is set by the user with the IC card being inserted in the right-of-copying/-listening data selling terminal 205, the set right-of-copying/-listening data will be written to the IC card. At the same time, the copying/reproduction log stored in the IC card are taken up by the right-of-copying/-listening data selling terminal 205 while the copying/reproduction log in the IC card is cleared.

[0137] In the above-mentioned embodiment of the billing system, in case an operation needing a billing is set as the recording or reproduction rule, the security decoder 17 in the data recorder/player 10 will make a billing for a data copying or reproduction.

[0138] FIG. 12 shows a flow of operations made in step S49 when the recording rule is set in step S48 for application to a billing-based copying.

[0139] First, a remaining number of times copying can

be done included in the right-of-copying data in the memory in the security decoder 17 is checked to judge whether the billing operation is possible (in step S81). When it is judged in step S81 that the billing is possible, the recording (copying) is effected (in step S82). When it is made sure that the recording is complete (in step S83), the number of times copying can be done included in the right-of-copying data in the memory of the security decoder 17 is decremented (in step S84). As copying log, information such as identifier for a copied musical content, type of the content, number of times of copying, copying time, etc. is stored into the memory (in step S85) and the billing is ended.

[0140] On the other hand, if it is judged in step S81 that no billing is possible since there remains no number of times copying can be done included in the right-of-copying data in the memory of the security decoder 17, the user is informed of the fact by displaying a message telling that there remains no number of times copying can be done in the right-of-copying data (in step S86). It is judged whether right-of-copying data has been added (in step S87). When the right-of-copying data has been added, the operation goes to step S82 where recording will be done and operations in step S83 and subsequent steps be effected. If it is judged in step S87 that there has not been added any right-of-copying data, it is judged that recording is impossible (in step S88), and the billing routine is ended.

[0141] FIG. 13 a flow of operations made in step S74 when the reproduction rule is set in step S73 to be applied to a billing-based copying.

[0142] First, a permitted number of times listening can be done included in the right-of-listening data in the memory in the security decoder 17 is checked to judge whether the billing is possible (in step S91). When it is judged in step S91 that the billing can be done, data to be reproduced are decoded for decryption (in step S92). When it is made sure that the decoding is complete (in step S93), the number of times listening can be done included in the right-of-listening data in the memory of the security decoder 17 is decremented (in step S94). As reproduction log, information such as identifier for a reproduced musical content, type of the content, number of times of reproduction, reproducing time, etc. is stored into the memory (in step S95) and the billing is ended.

[0143] On the other hand, if it is judged in step S91 that no billing is possible since there remains no number of times listening can be done in the right-of-listening data in the memory of the security decoder 17, the user is informed of the fact by displaying a message telling that there remains no number of times listening can be done in the right-of-listening data (in step S96). It is judged whether right-of-listening data has been added (in step S97). When the right-of-listening data has been added, the operation goes to step S92 where decoding will be done and operations in step S93 and subsequent steps be effected. If it is judged in step S97 that there has not been added anyright-of-listening data, it is judged that decoding is impossible (in step S98), and the billing routine is ended.

[0144] Note that the system may be adapted so that in step S98, the reproduction is not completely inhibited but reproduction of only the most affecting passage or climax part is allowed.

[Other embodiments of the present invention]

[0145] The aforementioned first and second embodiments of the present invention are adapted to reproduce data even with the user ID module not connected to the data recorder/player or personal computer. However, an embodiment other than the above may be designed to reproduce main data only when the user ID module is connected. That is, any other embodiment may be constructed with the nonvolatile memory 14 being omitted so that to collate a user ID from the user ID module with a one detected from main data to be reproduced, the user ID module has to be connected also for data reproduction.

[0146] Also, any other embodiment may be designed to operate similarly to the above first and second embodiments but only after confirming the use by making sure that the connection of the user ID module is connected to the data recorder/player and collating a user ID stored in the nonvolatile memory 14 with a one from the user ID module.

[0147] For data recording in the aforementioned first and second embodiments, the user ID module are authenticated and vadlidated but no validation using a user ID is effected. However, when the user ID module is connected to the data recorder/player for data recording, a user ID may be used for authentication and validation of the user ID module.

[0148] The first and second embodiments concern the data recorder/player, but the present invention is also applicable to a recording-only device and playback-only device. In this case, the user ID module should be accessory to the recording-only device in any embodiments like the first and second ones. In a playback-only device, it suffices to register a user ID once in the nonvolatile memory and the user ID module has not to be kept connected to the player for data reproduction.

[0149] Of course, the above other embodiments may be modified in various manners.

[0150] Note that the registration of a user ID in the first and second embodiments is to register a user ID in a playback unit included in the data recorder/player 10. Namely, in the first and second embodiments, the user ID module should be connected to the recorder without fail to record the user ID. Therefore, in case only the recording unit is taken in consideration, it is not necessary to register any user ID.

[0151] However, in case the recording-only device or the function of the recording unit of the data recorder/player is dedicated to a specific user, a user ID may be

registered by the user ID module and stored in the nonvolatile memory to permit recording only when user IDs are coincident with each other.

[0152] The above embodiments use a user name or module ID as a use ID. In addition, they may be a fingerprint or voice print of the user or biometric information unique to each individual such as pulse as the user ID. In this case, a user ID such as biometric information stored in the nonvolatile memory and a one detected from data to be reproduced may be collate with each other in the player. Alternatively, no volatile memory nay be provided, and a user ID such as biometric information detected from main data to be reproduced and a one such as fingerprint, voice print or pulse, supplied from a biometric information input means may be collated with each other. In this case, the biometric information input means can use the user ID module.

[0153] Note that a commercially available recording medium such as a read-only type disc available from a recording company or the like should be handled as "ORIGINAL" and it is not owned by anyone as having previously been described. However, when data are copied from the "ORIGINAL" recording medium, a user ID will be buried in the copied data to identify the owner of the recording medium.

[0154] In the aforementioned embodiment, the user name is not specifically limited but it may be a personal name or a group name such as a family name. In short, a user name can be used in common within a range of "private use" prescribed in the Copyright Law.

[0155] By adapting a single recorder or player to register a plurality of user IDs therein, the single recorder or player can be used commonly by a plurality of users corresponding to the plurality of user IDs.

[0156] In the above embodiments, the user ID is buried in recorded. However, the user ID may of course be recorded in any area other than an area where the data are recorded. Also, when the recorded data are handled in units of file like computer data, the user ID can be added to the recorded data in units of a file.

[0157] In the above embodiments, when recording data, the user ID module 20 has to be connected to the data recorder/player 10. For data recording, however, a user ID (especially, a module ID) stored in the nonvolatile memory 14 of the data recorder/player 10 and a one carried by data to be recorded may be collated with each other by comparison without having to connect the user ID module 20 for data recording.

[0158] Also, the recording rule may be such that when the user ID stored in the nonvolatile memory 14 is coincident with a one carried by main data to be recorded, the user ID module 20 has not to be connected to the data recorder/player 10.

[0159] A user ID carried by the main data to be recorded does not only mean a one buried in the data to be recorded but also a one acquired from a TOC area of a recording medium or an area other than an area where the main data are to be recorded. Also, the user ID includes a one added at the top, middle or end of data downloaded from the Internet.

[0160] Of course, data to be recorded includes, not ones reproduced from a recording medium in the data recorder/player 10, ones supplied as analog or digital data. In this case, the input data may not be ones reproduced from a disc.

[0161] Note that in the above embodiments, the audio data have been taken as the example of a content to be recorded but they may be any contents whose copyrights have to be managed such as video data and programs, game programs and data, etc.

[0162] The recording medium is not limited to any disc but may be a card type memory, semiconductor memory, hard disc used in a hard disc drive, etc. Further, data to be recorded are not limited to ones reproduced from a recording medium as above, but may be ones sent via a cable telephone line, radio telephone line or Internet.

Industrial Applicability

[0163] According to the present invention, for data recording, a registered user ID is recorded along with main data to be recorded while for data reproduction, a user ID available from the nonvolatile memory 14 is compared with a user ID detected from data read from a recording medium. When the user IDs are coincident with each other, the main data can be normally reproduced. Thus, it is permitted to copy the main data only for a private use.

Claims

1. A method of recording and/or reproducing data to a recording medium, comprising steps of:

   comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for recording or reproduction of the main data to or from the recording medium; and
   recording or reproducing the main data to or from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

2. The method according to claim 1, wherein:

   the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and
   data are recorded to or reproduced from the recording medium based the management data read from the recording medium when the user

identification data read from the recording medium is not coincident with that read from the data recorder/player.

3. The method according to claim 1, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded to the recording medium.

4. The method according to claim 3, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium.

5. The method according to claim 3, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium.

6. The method according to claim 1, wherein:

the recording medium has further recorded therein a management data to manage recording to or reproduction from the recording medium; and
main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

7. The method according to claim 6, further comprising a step of permitting the data reproduction from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a specific identification data.

8. The method according to claim 7, wherein the specific identification data indicates that the recording medium is an original one.

9. The method according to claim 1, wherein the user identification data read from the data recorder/player is set by the user.

10. The method according to claim 9, wherein the user identification data is a data including a user name.

11. A method of recording data to a recording medium, comprising steps of:

comparing a user identification data read from a recording medium having recorded the user identification data along with main data, with a one read from a data recorder/player, for recording the main data to the recording medium; and
recording the main data to the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

12. The method according to claim 11, wherein:

the recording medium has further recorded therein a management data to manage recording to the recording medium; and
main data are recorded to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

13. The method according to claim 11, where when the user identification data read from the recording medium is coincident with that read from the data recorder/player, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded to the recording medium.

14. The method according to claim 13, wherein the user identification data read from the data recorder/player is buried in main data to be recorded to the recording medium.

15. The method according to claim 14, wherein the user identification data read from the data recorder/player is encrypted and buried in main data to be recorded to the recording medium.

16. The method according to claim 11, wherein the user-identification data read from the data recorder/player is set by the user.

17. The method according to claim 16, wherein the user identification data includes a user name.

18. A recording-medium recorder comprising:

a head to scan a recording medium having stored therein a user identification data along with main data;
a memory having a user identification data recorded therein; and
a controller to compare the user identification data read by the head from the recording me-

dium with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

19. The apparatus according to claim 18, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller controls the head to record main data to the recording medium.

20. The apparatus according to claim 18, wherein the memory is provided in a user identification data server connected to the data recorder/player.

21. The apparatus according to claim 20, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.

22. The apparatus according to claim 21, wherein when the authentication has successfully be made made, the controller instructs the user identification data server to read the user identification data from the memory.

23. The apparatus according to claim 22, wherein the user identification data read from the memory is encrypted and sent from the user identification data server to the controller.

24. The apparatus according to claim 21, wherein when the authentication has not successfully be made, the controller ceases the operations of recording to the recording medium.

25. The apparatus according to claim 21, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.

26. The apparatus according to claim 19, wherein:

the recording medium has further recorded therein a management data to manage recording to the recording medium; and
the controller records main data to the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the memory.

27. The apparatus according to claim 26, where when the user identification data read from the recording medium is coincident with that read from the memory, main data to be recorded to the recording medium are encrypted with the user identification data read from the data recorder/player being taken as an encryption key and then recorded by the head to the recording medium.

28. The apparatus according to claim 27, wherein the user identification data read from the memory is buried in main data to be recorded to the recording medium.

29. The method according to claim 28, wherein the controller encrypts the user identification data read from the memory and buries it in main data to be recorded to the recording medium.

30. The apparatus according to claim 18, wherein a user identification data set by the user is written to the memory.

31. The apparatus according to claim 18, wherein the user identification data to be stored into the memory is set by the user.

32. The apparatus according to claim 31, wherein the user identification data includes a user name.

33. A recording-medium playback method, comprising steps of:

comparing a user identification data read from a recording medium having recorded therein the user identification data along with main data, with a one read from a data recorder/player, for reproducing the main data from the recording medium; and
reproducing the main data from the recording medium when the user identification data read from the recording medium is coincident with a one read from the data recorder/player.

34. The method according to claim 33, wherein:

the recording medium has further recorded therein a management data to manage the operations of data reproduction from the recording medium; and
main data are reproduced from the recording medium based the management data read from the recording medium when the user identification data read from the recording medium is not coincident with that read from the data recorder/player.

35. The method according to claim 34, wherein when the user identification data read from the recording medium is not coincident with that read from the data recorder/player and also when the user identification data read from the recording medium is a

specific identification data, playback of the recording medium is allowed.

36. The method according to claim 35, wherein the specific identification data indicates that the recording medium is an original one.

37. The method according to claim 33, wherein:

the recording medium has encrypted data recorded therein; and
main data read from the recording medium are decrypted using, as an encryption key, the user identification data read from the recording medium when the user identification data read from the recording medium is coincident with that read from the data recorder/player.

38. The method according to claim 33, wherein the user identification data read from the data recorder/player is set by the user.

39. The method according to claim 38, wherein the user identification data includes a user name.

40. A recording-medium player comprising:

a head to scan a recording medium having recorded therein encrypted data as well as at least a user identification data and reproduction management data;
a memory having a user identification data stored therein; and
a controller to compare the user identification data read by the head from the recording medium, with that read from the memory and control operations for playback of the recording medium on the basis of the result of comparison.

41. The apparatus according to claim 40, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller allows to reproduce main data from the recording medium.

42. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is coincident with that read from the memory, the controller decrypts main data read by the head from the recording medium using the user identification data.

43. The apparatus according to claim 42, wherein when the user identification data read by the head from the recording medium cannot be detected, the controller controls the operations for playback of the recording medium based on the reproduction management data read from the recording medium.

44. The apparatus according to claim 40, wherein the memory is provided in a user identification data server connected to the data recorder/player.

45. The apparatus according to claim 40, wherein the controller makes mutual authentication with the user identification data server when it is judged that the latter is connected to the data recorder/player.

46. The apparatus according to claim 45, wherein when the authentication has successfully be made, the controller instructs the user identification data server to read the user identification data from the memory.

47. The apparatus according to claim 46, wherein the user identification data read from the memory is encrypted and sent from the user identification data server.

48. The apparatus according to claim 45, wherein when the authentication has not successfully be made, the controller ceases the operations for data reproduction from the recording medium.

49. The apparatus according to claim 40, wherein when it is judged that the user identification data server is not connected to the data recorder/player, the controller prompts the user to connect the user identification data server to the data recorder/player.

50. The apparatus according to claim 41, wherein when the user identification data read from the recording medium is not coincident with that read from the memory and also when the user identification data read from the recording medium is a specific identification data, the controller allows to reproduce data from the recording medium.

51. The apparatus according to claim 50, wherein the specific identification data indicates the recording medium is an original one.

52. The apparatus according to claim 50, wherein the user identification data set by the user is written to the memory.

53. The apparatus according to claim 40, wherein the user identification data read from the recording medium is set by the user.

54. The apparatus according to claim 53, wherein the user identification data includes a user name.

55. A method of controlling data copying, comprising steps of:

comparing a user identification data read from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for copying the main data; and controlling data output when the user identification data extracted from the data is coincident with that read from the data recorder/player.

56. The method according to claim 55, wherein:

the main data further includes a management data to manage the operations of copying the data; and
the data copying is controlled based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

57. The method according to claim 56, wherein when the user identification data extracted from the main data is coincident with that read from the data recorder/player, the user identification data extracted from the main data is encrypted using the user identification data as an encryption key before being outputted.

58. The method according to claim 57, wherein the user identification data read from the data recorder/player is buried in the main data.

59. The method according to claim 57, wherein the user identification data read from the data recorder/player is encrypted and buried into the main data.

60. The method according to claim 56, wherein when the management data indicates that billing has to be done for copying the main data, it is judged whether the billing is possible, and the copying is done when the result of judgment is that the billing is possible.

61. The method according to claim 60, wherein the billing is such that a number of times main data can be copied is decremented.

62. The method according to claim 61, wherein when it is judged that the billing is not possible and also when the number of times main data can be copied is not incremented, the copying operation is ceased.

63. The method according to claim 55, wherein the user identification data read from the data recorder/player is set by the user.

64. The method according to claim 63, wherein the user identification data includes a user name.

65. A data reproducing method comprising steps of:

comparing a user identification data extracted from main data having at least the user identification data buried therein, with a one read from a data recorder/player, for reproduction of the main data; and
reproducing the main data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

66. The method according to claim 65, wherein:

the main data further includes a management data to manage the operation of reproducing the main data; and
the main data are reproduced based on the management data when the user identification data extracted from the main data is not coincident with that read from the data recorder/player.

67. The method according to claim 66, wherein when the user identification data cannot be detected from the main data, the operation of reproducing the main data is controlled based on the management data.

68. The method according to claim 66, wherein when the user identification data extracted from the main data is not coincident with that read from the data recorder/player and also when the user identification data extracted from the main data is a specific identification data, it is allowed to reproduce the main data.

69. The method according to claim 68, wherein the specific identification data indicates that the recording medium is an original one.

70. The method according to claim 66, wherein when the management data indicates that billing has to be done for reproduction of the main data, it is judged whether the billing is possible, and the main data are reproduced when the result of judgment is that the billing is possible.

71. The method according to claim 70, wherein the billing is made by decrementing a number of times the reproduction can be done.

72. The method according to claim 71, wherein when it is judged that the billing is not possible and also when the number of times of reproduction is not incremented, the operation of reproduction is inhibit-

ed.

73. The method according to claim 65, wherein:

the main data includes encrypted data; and the user identification data extracted from the main data is decrypted using the user identification data when the user identification data extracted from the main data is coincident with that read from the data recorder/player.

74. The method according to claim 65, wherein the user identification data read from the data recorder/player is set by the user.

75. The method according to claim 74, wherein the user identification data includes a user name.

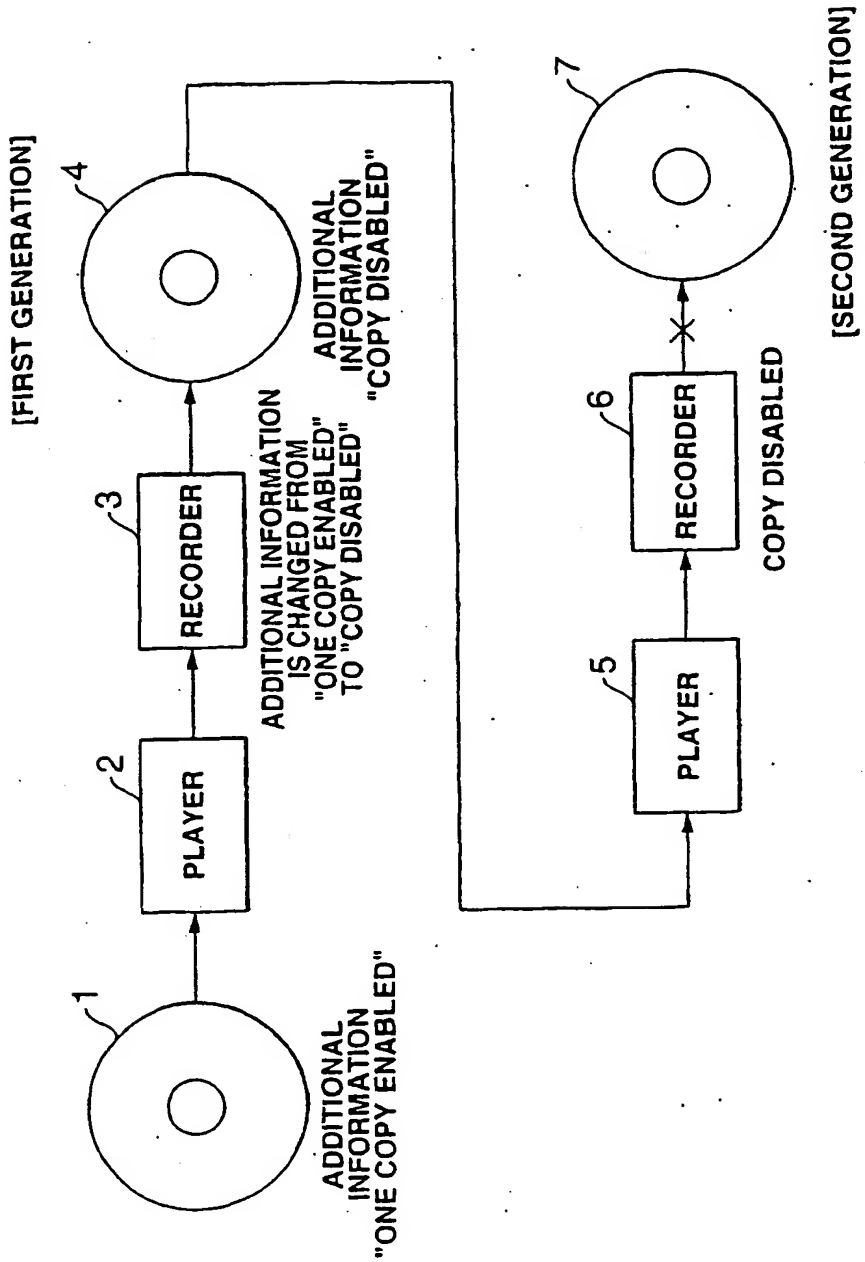

[FIRST GENERATION]
1
ADDITIONAL INFORMATION "ONE COPY ENABLED"
2
PLAYER
3
RECORDER
ADDITIONAL INFORMATION IS CHANGED FROM "ONE COPY ENABLED" TO "COPY DISABLED"
4
ADDITIONAL INFORMATION "COPY DISABLED"
5
PLAYER
6
RECORDER
COPY DISABLED
7
[SECOND GENERATION]

FIG.1

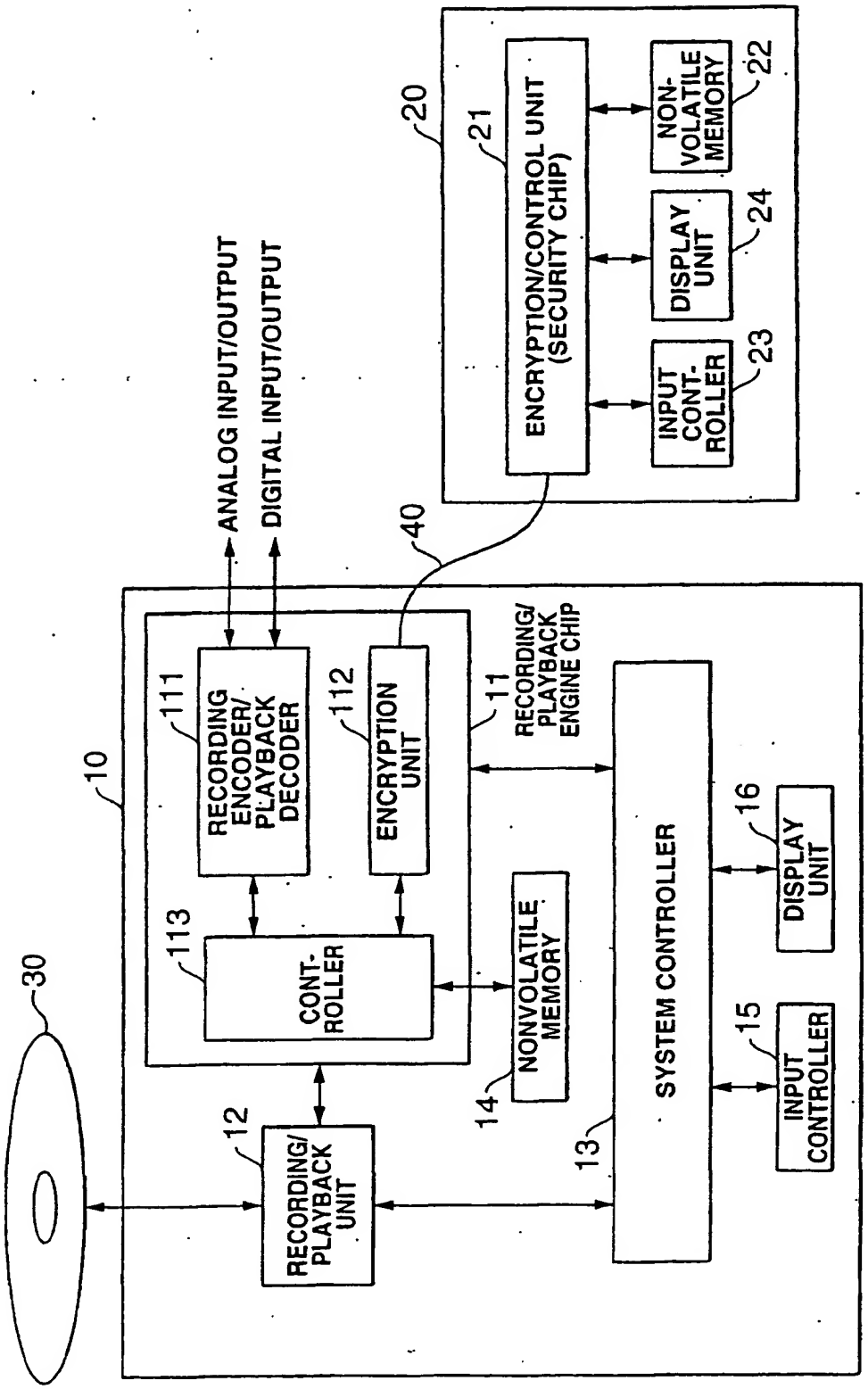

30
10
12
RECORDING/ PLAYBACK UNIT
111
RECORDING ENCODER/ PLAYBACK DECODER
112
ENCRYPTION UNIT
113
CONT-ROLLER
11
RECORDING/ PLAYBACK ENGINE CHIP
14
NONVOLATILE MEMORY
13
SYSTEM CONTROLLER
15
INPUT CONTROLLER
16
DISPLAY UNIT
ANALOG INPUT/OUTPUT
DIGITAL INPUT/OUTPUT
40
20
21
ENCRYPTION/CONTROL UNIT (SECURITY CHIP)
22
NON-VOLATILE MEMORY
24
DISPLAY UNIT
23
INPUT CONT-ROLLER

FIG.2

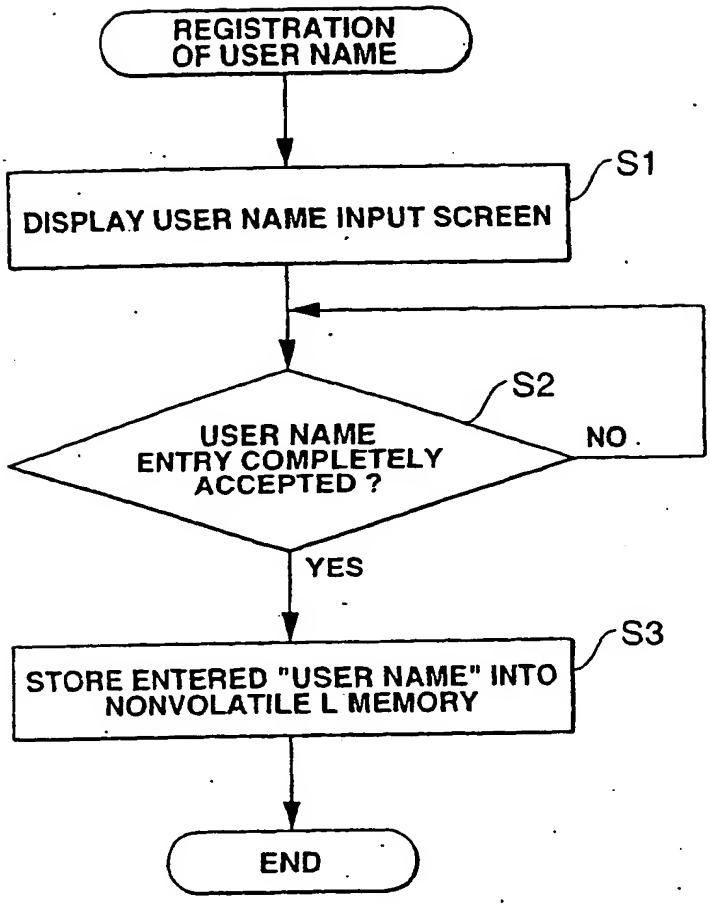

REGISTRATION OF USER NAME
S1
DISPLAY USER NAME INPUT SCREEN
S2
USER NAME ENTRY COMPLETELY ACCEPTED ?
NO
YES
S3
STORE ENTERED "USER NAME" INTO NONVOLATILE L MEMORY
END

FIG.3

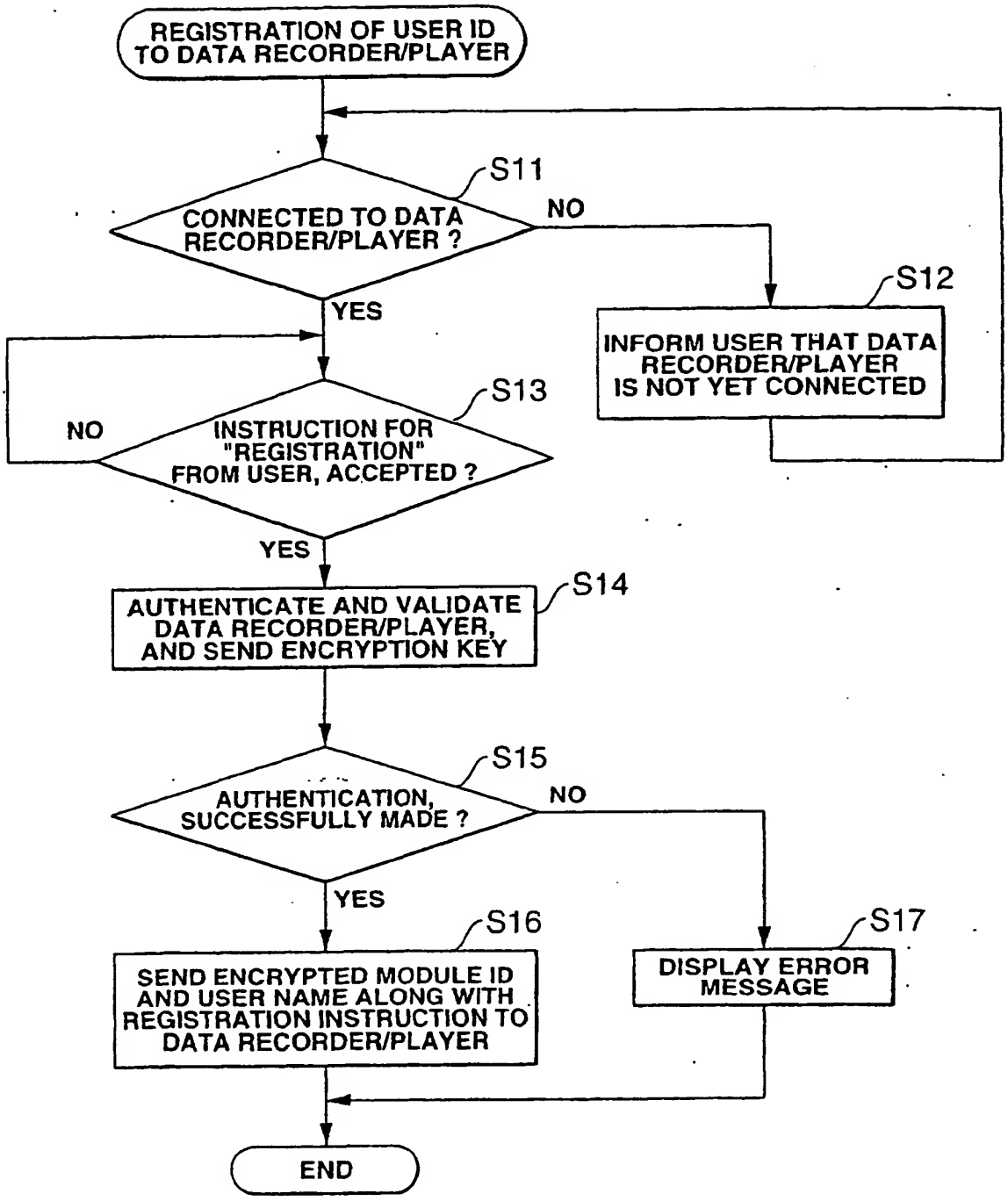

REGISTRATION OF USER ID TO DATA RECORDER/PLAYER
S11
CONNECTED TO DATA RECORDER/PLAYER ?
NO
S12
INFORM USER THAT DATA RECORDER/PLAYER IS NOT YET CONNECTED
YES
S13
NO
INSTRUCTION FOR "REGISTRATION" FROM USER, ACCEPTED ?
YES
S14
AUTHENTICATE AND VALIDATE DATA RECORDER/PLAYER, AND SEND ENCRYPTION KEY
S15
AUTHENTICATION, SUCCESSFULLY MADE ?
NO
YES
S16
SEND ENCRYPTED MODULE ID AND USER NAME ALONG WITH REGISTRATION INSTRUCTION TO DATA RECORDER/PLAYER
S17
DISPLAY ERROR MESSAGE
END

FIG.4

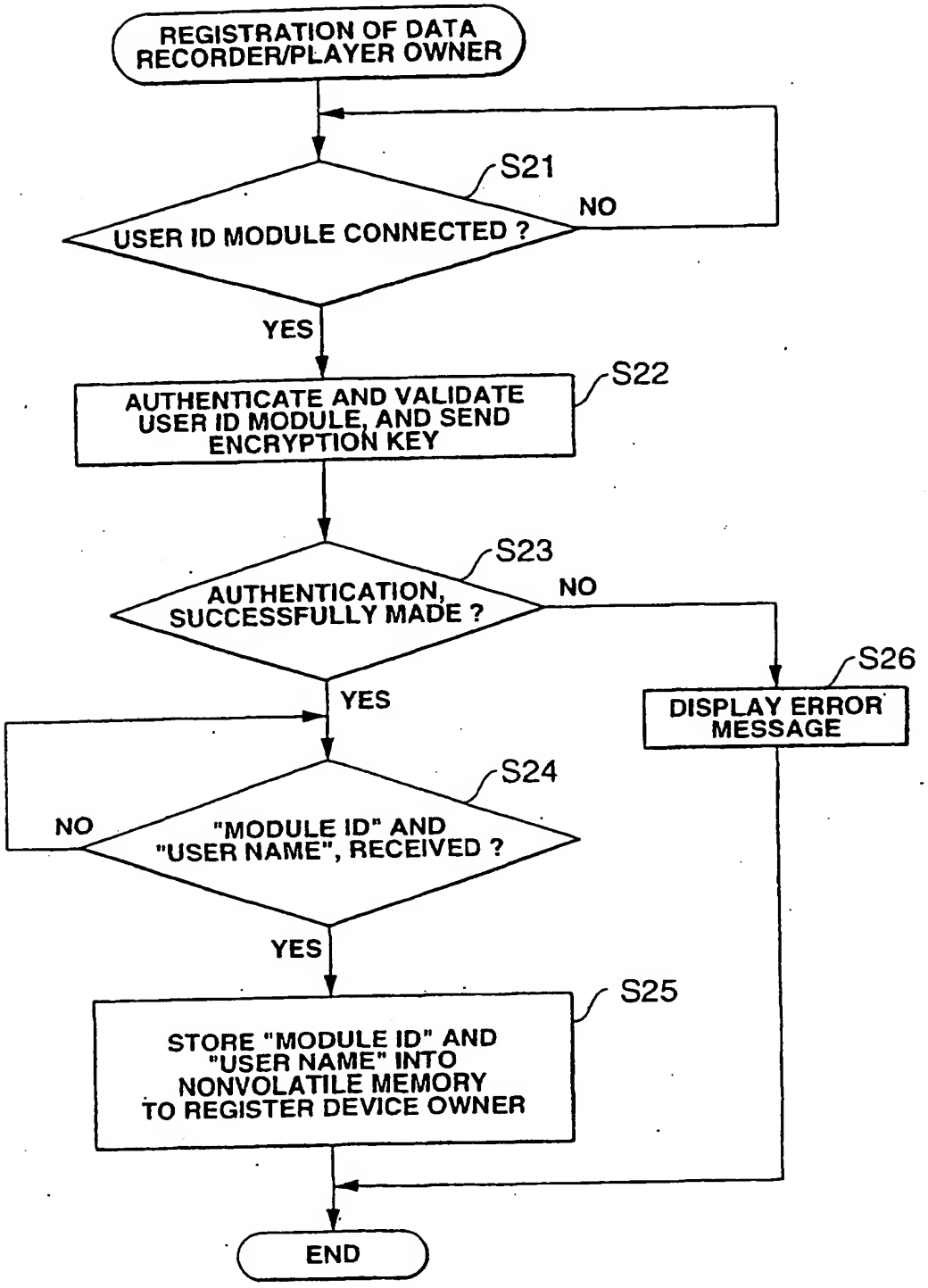

REGISTRATION OF DATA RECORDER/PLAYER OWNER
S21
USER ID MODULE CONNECTED ?
NO
YES
S22
AUTHENTICATE AND VALIDATE USER ID MODULE, AND SEND ENCRYPTION KEY
S23
AUTHENTICATION, SUCCESSFULLY MADE ?
NO
YES
S26
DISPLAY ERROR MESSAGE
S24
NO
"MODULE ID" AND "USER NAME", RECEIVED ?
YES
S25
STORE "MODULE ID" AND "USER NAME" INTO NONVOLATILE MEMORY TO REGISTER DEVICE OWNER
END

FIG.5

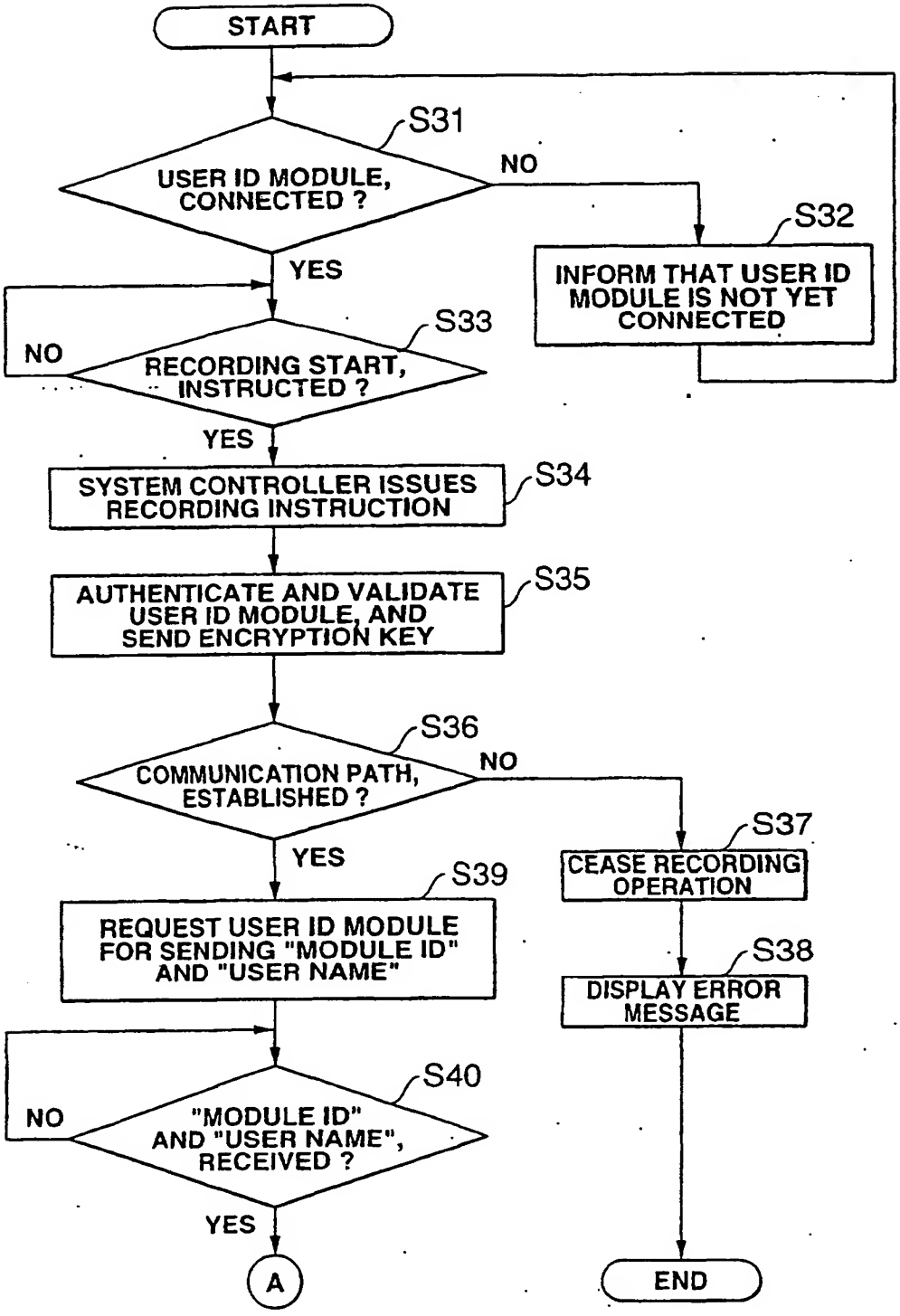

START
S31
USER ID MODULE, CONNECTED ?
NO
S32
INFORM THAT USER ID MODULE IS NOT YET CONNECTED
YES
S33
NO
RECORDING START, INSTRUCTED ?
YES
SYSTEM CONTROLLER ISSUES RECORDING INSTRUCTION
S34
AUTHENTICATE AND VALIDATE USER ID MODULE, AND SEND ENCRYPTION KEY
S35
S36
COMMUNICATION PATH, ESTABLISHED ?
NO
S37
CEASE RECORDING OPERATION
YES
S39
REQUEST USER ID MODULE FOR SENDING "MODULE ID" AND "USER NAME"
S38
DISPLAY ERROR MESSAGE
S40
NO
"MODULE ID" AND "USER NAME", RECEIVED ?
YES
A
END

FIG.6

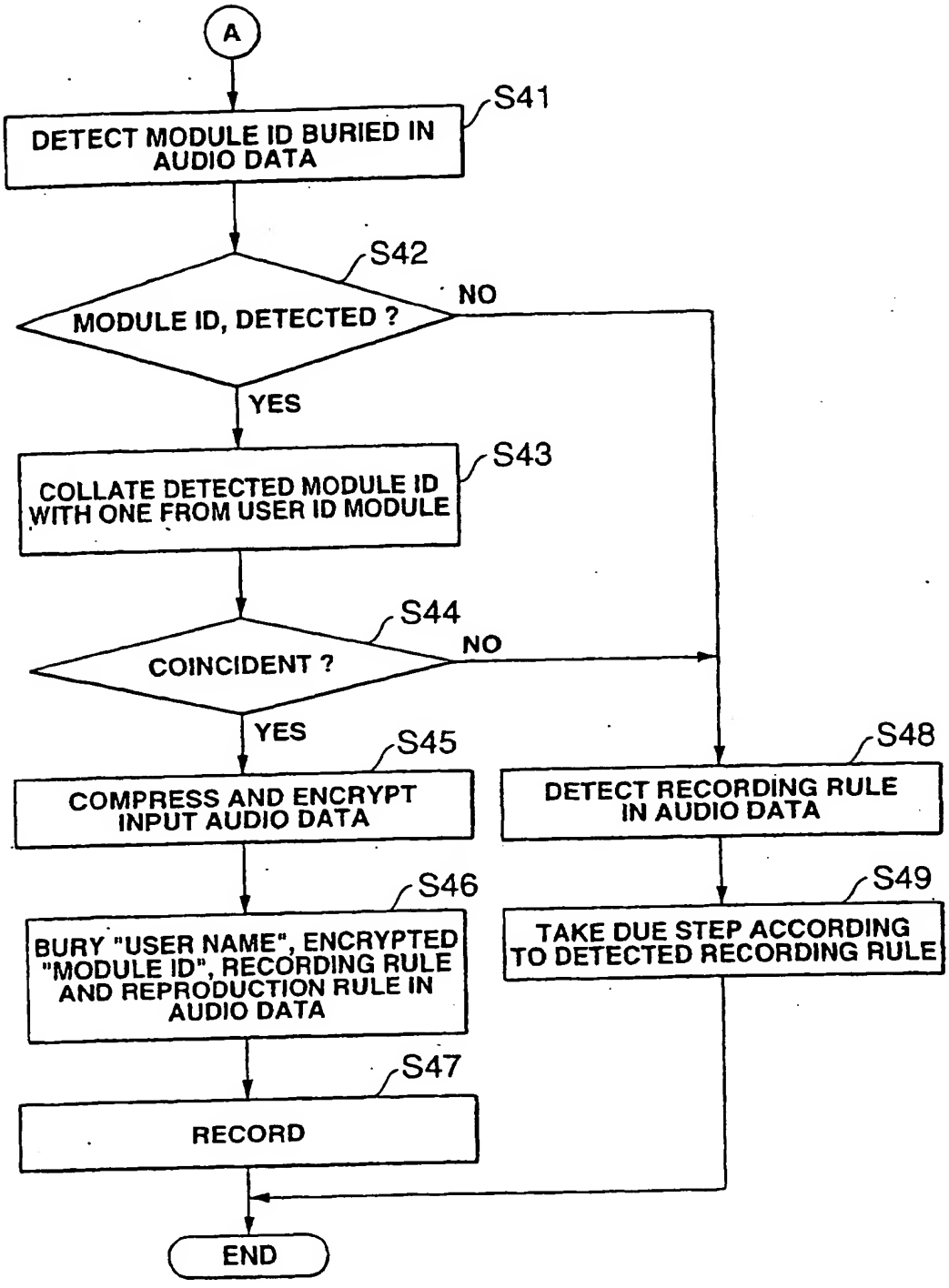

A
S41
DETECT MODULE ID BURIED IN AUDIO DATA
S42
MODULE ID, DETECTED ?
NO
YES
S43
COLLATE DETECTED MODULE ID WITH ONE FROM USER ID MODULE
S44
COINCIDENT ?
NO
YES
S45
COMPRESS AND ENCRYPT INPUT AUDIO DATA
S46
BURY "USER NAME", ENCRYPTED "MODULE ID", RECORDING RULE AND REPRODUCTION RULE IN AUDIO DATA
S47
RECORD
S48
DETECT RECORDING RULE IN AUDIO DATA
S49
TAKE DUE STEP ACCORDING TO DETECTED RECORDING RULE
END

FIG.7

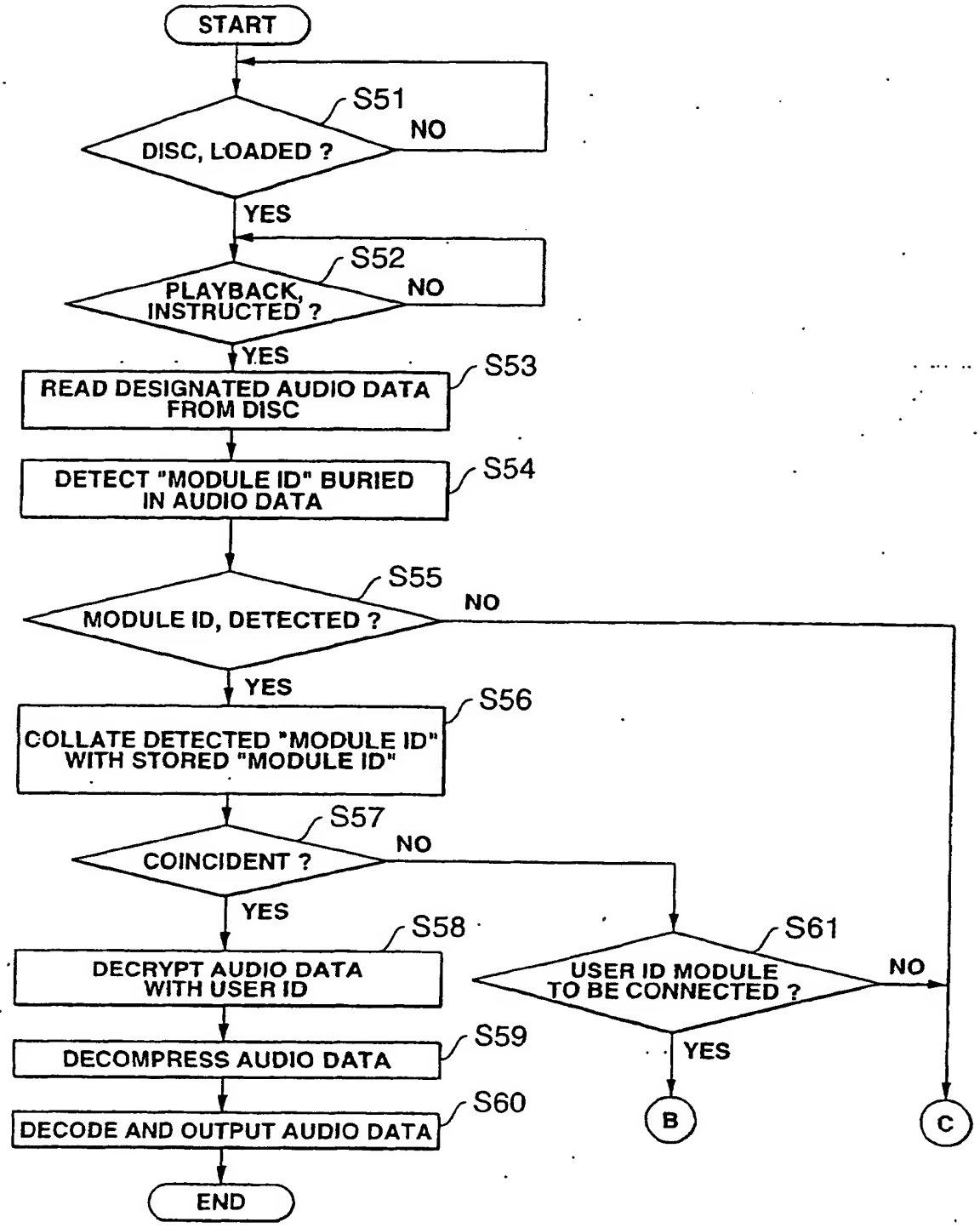

START
S51
DISC, LOADED ?
NO
YES
S52
PLAYBACK, INSTRUCTED ?
NO
YES
S53
READ DESIGNATED AUDIO DATA FROM DISC
S54
DETECT "MODULE ID" BURIED IN AUDIO DATA
S55
MODULE ID, DETECTED ?
NO
YES
S56
COLLATE DETECTED "MODULE ID" WITH STORED "MODULE ID"
S57
COINCIDENT ?
NO
YES
S58
DECRYPT AUDIO DATA WITH USER ID
S59
DECOMPRESS AUDIO DATA
S60
DECODE AND OUTPUT AUDIO DATA
END
S61
USER ID MODULE TO BE CONNECTED ?
NO
YES
B
C

FIG.8

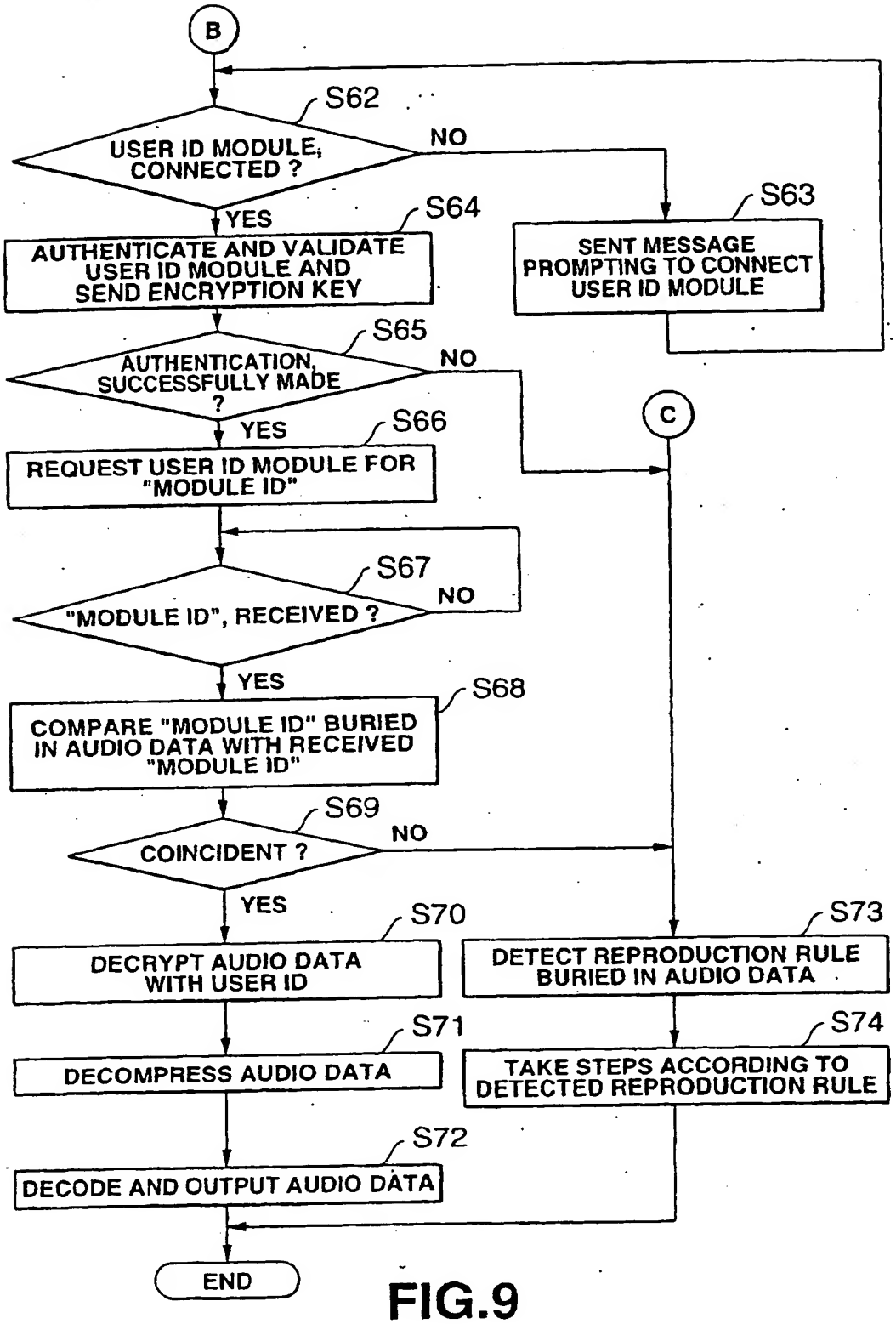

B
S62
USER ID MODULE, CONNECTED ?
NO
YES
S63
SENT MESSAGE PROMPTING TO CONNECT USER ID MODULE
S64
AUTHENTICATE AND VALIDATE USER ID MODULE AND SEND ENCRYPTION KEY
S65
AUTHENTICATION, SUCCESSFULLY MADE ?
NO
YES
C
S66
REQUEST USER ID MODULE FOR "MODULE ID"
S67
"MODULE ID", RECEIVED ?
NO
YES
S68
COMPARE "MODULE ID" BURIED IN AUDIO DATA WITH RECEIVED "MODULE ID"
S69
COINCIDENT ?
NO
YES
S70
DECRYPT AUDIO DATA WITH USER ID
S73
DETECT REPRODUCTION RULE BURIED IN AUDIO DATA
S71
DECOMPRESS AUDIO DATA
S74
TAKE STEPS ACCORDING TO DETECTED REPRODUCTION RULE
S72
DECODE AND OUTPUT AUDIO DATA
END

FIG.9

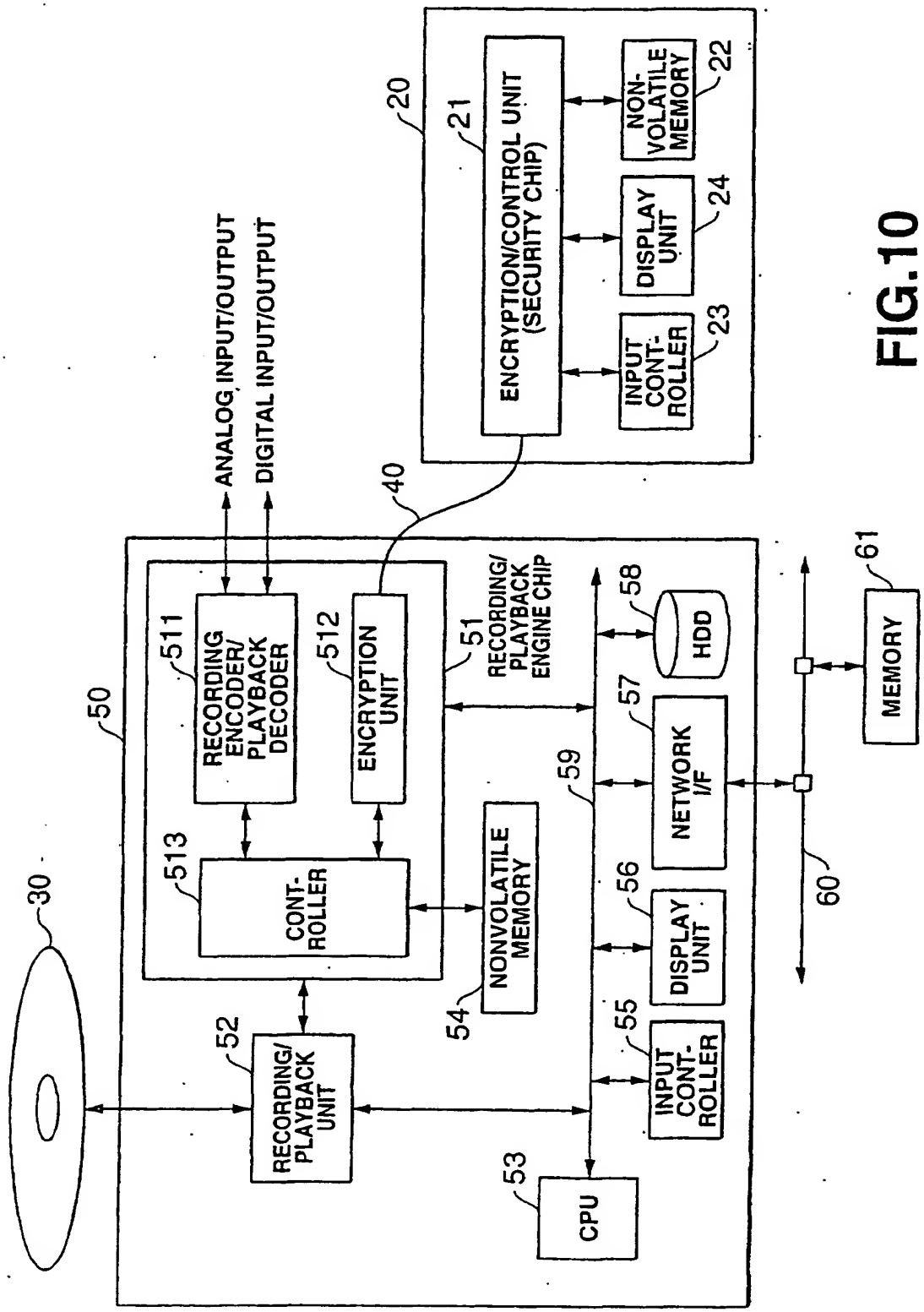

20
21
ENCRYPTION/CONTROL UNIT (SECURITY CHIP)
NON-VOLATILE MEMORY
22
DISPLAY UNIT
24
INPUT CONT-ROLLER
23
40
ANALOG INPUT/OUTPUT
DIGITAL INPUT/OUTPUT
50
RECORDING ENCODER/ PLAYBACK DECODER
511
ENCRYPTION UNIT
512
51
RECORDING/ PLAYBACK ENGINE CHIP
58
HDD
61
MEMORY
57
NETWORK I/F
59
513
CONT-ROLLER
NONVOLATILE MEMORY
54
56
DISPLAY UNIT
60
30
52
RECORDING/ PLAYBACK UNIT
55
INPUT CONT-ROLLER
53
CPU

FIG.10

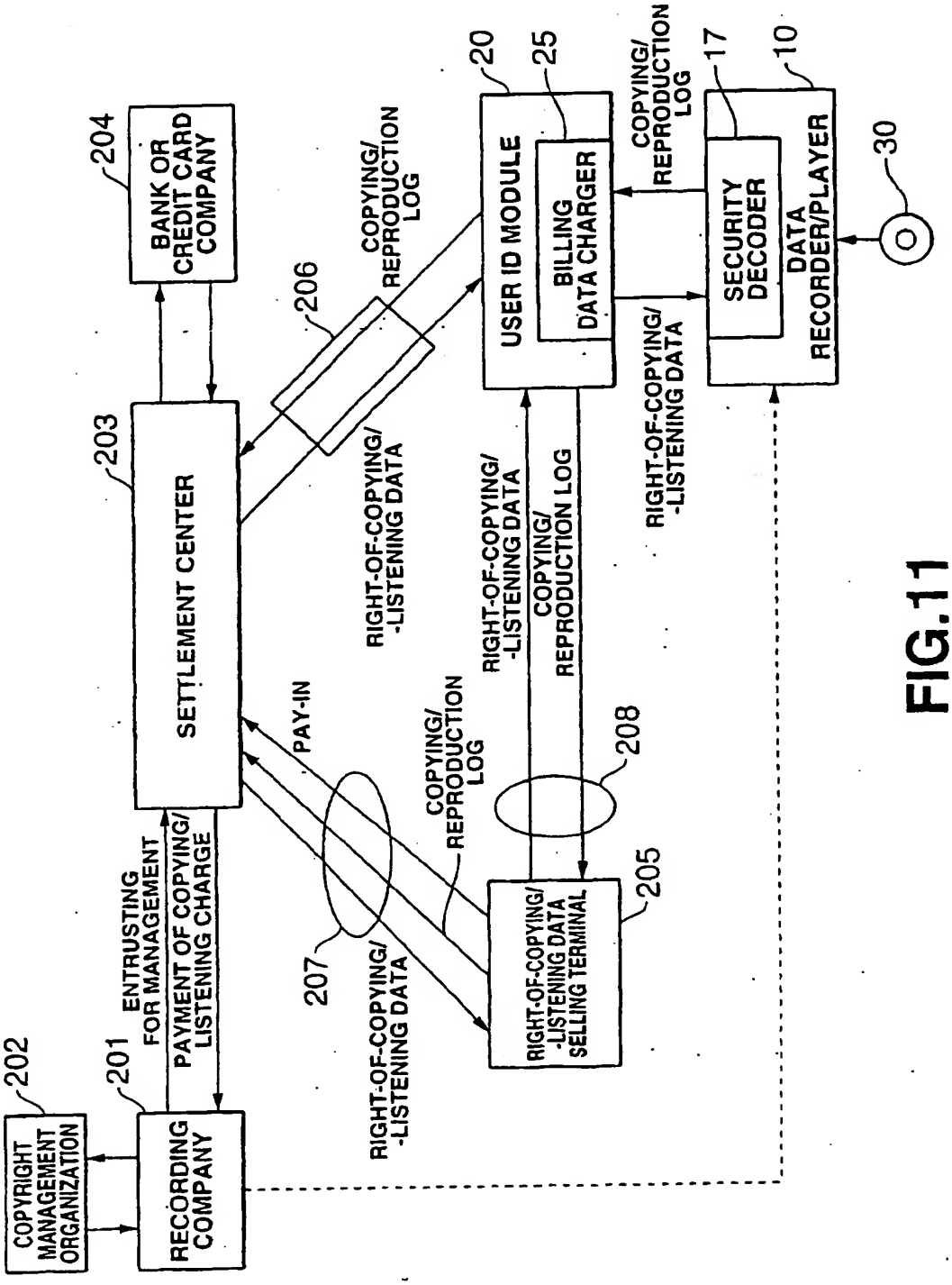

COPYRIGHT MANAGEMENT ORGANIZATION
202
RECORDING COMPANY
201
ENTRUSTING FOR MANAGEMENT
PAYMENT OF COPYING/ LISTENING CHARGE
BANK OR CREDIT CARD COMPANY
204
SETTLEMENT CENTER
203
PAY-IN
206
COPYING/ REPRODUCTION LOG
RIGHT-OF-COPYING/ -LISTENING DATA
207
RIGHT-OF-COPYING/ -LISTENING DATA SELLING TERMINAL
205
208
USER ID MODULE
20
BILLING DATA CHARGER
25
SECURITY DECODER
17
DATA RECORDER/PLAYER
10
30

FIG.11

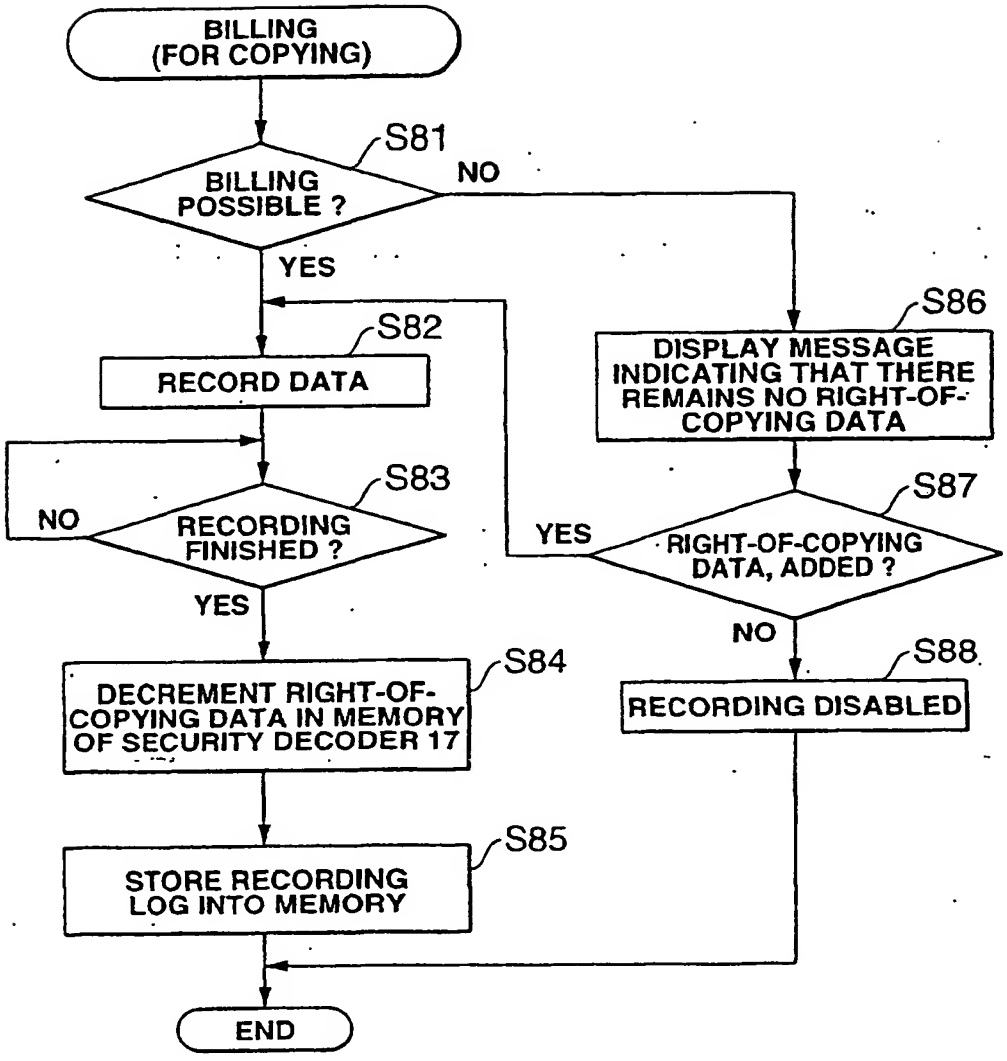

BILLING (FOR COPYING)
S81
BILLING POSSIBLE ?
NO
YES
S82
RECORD DATA
S83
NO
RECORDING FINISHED ?
YES
S84
DECREMENT RIGHT-OF-COPYING DATA IN MEMORY OF SECURITY DECODER 17
S85
STORE RECORDING LOG INTO MEMORY
END
S86
DISPLAY MESSAGE INDICATING THAT THERE REMAINS NO RIGHT-OF-COPYING DATA
S87
YES
RIGHT-OF-COPYING DATA, ADDED ?
NO
S88
RECORDING DISABLED

FIG.12

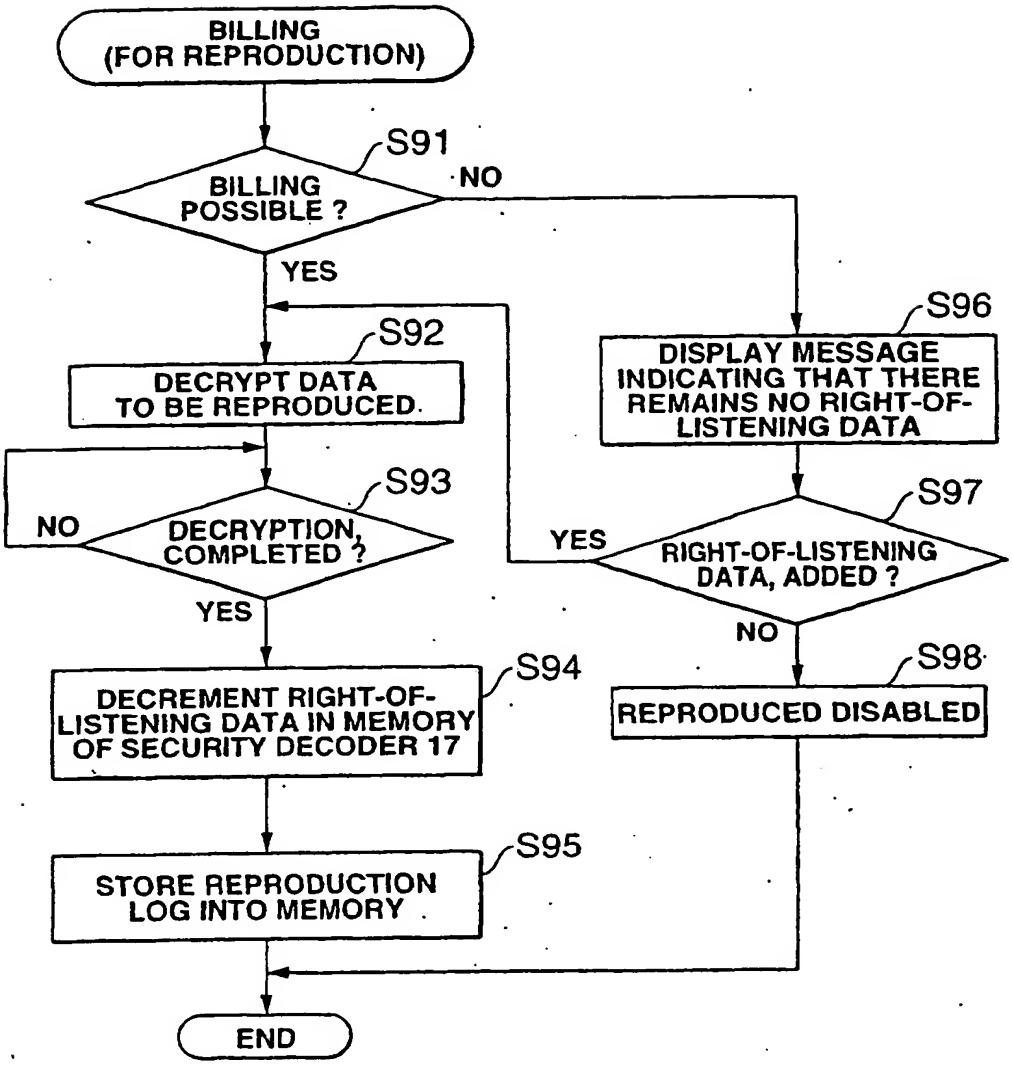

BILLING
(FOR REPRODUCTION)
S91
BILLING POSSIBLE ?
NO
YES
S92
DECRYPT DATA TO BE REPRODUCED
S93
NO
DECRYPTION, COMPLETED ?
YES
S94
DECREMENT RIGHT-OF-LISTENING DATA IN MEMORY OF SECURITY DECODER 17
S95
STORE REPRODUCTION LOG INTO MEMORY
END
S96
DISPLAY MESSAGE INDICATING THAT THERE REMAINS NO RIGHT-OF-LISTENING DATA
S97
YES
RIGHT-OF-LISTENING DATA, ADDED ?
NO
S98
REPRODUCED DISABLED

FIG.13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/06183

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B 20/10, G10F 3/06, G06F 17/60, G10K 15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B 20/10, H04N 5/91, G10F 3/06, G06F 17/60, G10K 15/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-238306 A (Fujitsu Limited), 31 August, 1999 (31.08.99), Full text; Figs. 1 to 18 & EP 000930616 A2 & CN 001227948 A	1-75
Y	JP 10-208388 A (Victor Company of Japan, Limited), 07 August, 1998 (07.08.98), Full text; Figs. 1 to 7 & EP 000853315 A2 & US 006097814 A1	1-75
Y	JP 11-306672 A (Sony Corporation), 05 November, 1999 (05.11.99), Full text; Figs. 1 to 8 (Family: none)	1-75
Y	JP 2000-113587 A (Sony Corporation), 21 April, 2000 (21.04.00), Full text; Figs. 1 to 10 (Family: none)	1-75
A	JP 2000-195161 A (Victor Company of Japan, Limited), 14 July, 2000 (14.07.00), Full text; Figs. 1 to 11 (Family: none)	1-75

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 October, 2001 (03.10.01)	16 October, 2001 (16.10.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/06183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-213554 A (Toshiba Corporation), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 22 & CN 001220460 A	7-8,35-36, 50-51,68-69
A	JP 2000-156036 A (Sony Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 1 to 5 (Family: none)	20-25,44-49
A	JP 11-313282 A (Sanyo Electric Co., Ltd.), 09 November, 1999 (09.11.99), Full text; Figs. 1 to 16 & EP 000954173 A1	60-62,70-72

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年1 月24 日 (24.01.2002)

PCT

(10) 国際公開番号
WO 02/07161 A1

(51) 国際特許分類[7]: G11B 20/10, G10F 3/06, G06F 17/60, G10K 15/02

(21) 国際出願番号: PCT/JP01/06183

(22) 国際出願日: 2001 年7 月17 日 (17.07.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-216388 2000 年7 月17 日 (17.07.2000) JP
特願2000-260467 2000 年8 月30 日 (30.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 猪口達也 (INOKUCHI, Tatsuya) [JP/JP]. 佐古曜一郎 (SAKO, Yoichiro) [JP/JP]. 鳥山 充 (TORIYAMA, Mitsuru) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

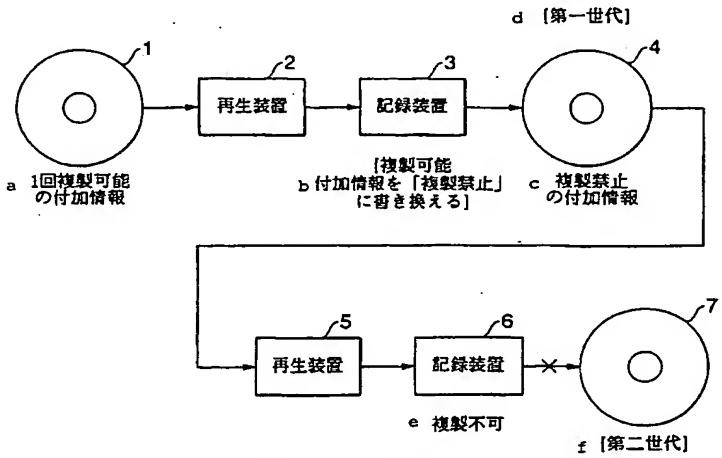
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: METHOD AND APPARATUS FOR RECORDING AND/OR REPRODUCING DATA AND RECORD MEDIUM

(54) 発明の名称: データ記録及び／又は再生方法及び装置並びに記録媒体



a...ADDITIONAL INFORMATION COPIABLE ONCE
b...[REWRITE COPIABLE ADDITIONAL INFORMATION TO "COPY PROHIBITED"]
c...COPY-PROHIBITED ADDITIONAL INFORMATION
d...[FIRST GENERATION]
e...NONCOPIABLE
f...[SECOND GENERATION]
2...REPRODUCER
3...RECORDER
5...REPRODUCER
6...RECORDER

(57) Abstract: A method for recording and/or reproducing data on and/or from a record medium, in which user identification data read out from a record medium where the user identification data along with data is recorded is compared with the user identification data read out from an apparatus in recording or reproducing data on or from the record medium. Recording or reproducing of the recording medium is performed when the user identification data read out from the record medium matches with the user identification data read out from the apparatus.

WO 02/07161 A1

[続葉有]

(57) 要約:

本発明は、記録媒体の記録及び／又は再生方法であり、データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された使用者識別データと記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、記録媒体から読み出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、記録媒体に記録又は再生を行う。

明細書

データ記録及び／又は再生方法及び装置並びに記録媒体

技術分野

本発明は、著作権管理が必要なコンテンツデータ、例えば、オーディオ情報、画像情報、ゲームプログラム及びデータ、コンピュータプログラムなどのデータを記録し、再生する方法及び記録及び／又は再生装置に関する。

背景技術

デジタルコンテンツの普及に伴い、このデジタルコンテンツについての不正な複製（コピー）による著作権侵害が問題となっている。すなわち、テープ媒体などへのアナログ記録の場合には、オーディオデータや画像データがアナログ的に記録されるため、複製を行うとデータの品質が劣化する。これに対し、デジタル的にオーディオデータや画像データを記録し再生する機器においては、原理的に複製によって情報品質が劣化することがなく、データの複製を多数回繰り返すことさえも品質の劣化無しに可能である。

そのため、デジタル的に処理を行う機器による不正コピーによる損害は、アナログの場合よりさらに大きなものとなり、デジタル的に処理を行う機器における不正コピー防止は、非常に重要になっている。

この問題に対処するため、デジタルコンテンツに複製制御のための情報を付加し、この付加情報を用いて、不正な複製を防止することが行われている。

例えば、この複製の防止のための制御として、オーディオコンテンツについては、１回は複製を認めるが、１回複製されたものからの複製を禁止するＳＣＭＳ（Serial Copy Management System ）と呼ばれる世代制限の複製制御方式による著作権保護施策が、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク（登録商標））、ＤＡＴ（デジタルオーディオテープ）などの装置において用いられてい

る。

このＳＣＭＳ方式の複製制御方式について、図１３を参照して説明する。

例えば、ディスク１には、オリジナルソースのオーディオ信号がデジタル記録されている。デジタルオーディオ信号は、ディスク１に、所定の記録フォーマットで記録されており、ＳＣＭＳ方式による１回複製可能を示す付加情報が、例えばデジタル信号中の特定のエリアに記録されている。

再生装置２は、ディスク１から読み出した信号からデジタルオーディオ信号を再生し、前記の付加情報と共に、記録装置３に伝送する。再生装置２では、通常再生速度（１倍速）に等しい時間分をかけて、デジタルオーディオ信号を記録装置３に伝送する。

このデジタルオーディオ信号を受け取った記録装置３は、デジタルオーディオ信号の付加情報が１回複製可能であるときには、入力デジタル信号の複製が可能であると認識する。記録装置３は、付加情報が１回複製可能であることを確認すると、記録可能なディスク４にデジタル信号を複製記録する。その際に、記録装置３は、付加情報を「１回複製可能」の状態から、「複製禁止」の状態に書き換える。したがって、ディスク４には、デジタル信号が複製記録が行われると共に、その付加情報として、「複製禁止」の情報が記録される。

この１回目の複製記録が行われたディスク４（第１世代のディスク）が再生装置５で再生されて、記録装置６に供給された場合、記録装置６では、付加情報が「複製禁止」となっていることを検知するので、記録可能なディスク７への記録はできなくなる。

このときの複製速度は、再生装置２からのオーディオ信号の伝送速度と等しくなり、オーディオ信号を標準再生時間で再生するとき、すなわち、ノーマル再生速度に等しい速度となる。

ここで、標準再生時間とは、オーディオ信号の場合、実時間再生速度であり、人間が通常知覚するときの再生速度である。例えば、データの場合、標準再生速度は各再生機器により決定され、人間の知覚に関わるものではない。

以上のようにして、ＳＣＭＳ方式では、記録装置で第１世代の複製は許可するが、第１世代の媒体からの第２世代の複製はできないように制御して、著作権保

護を行っている。

ＳＣＭＳ方式の本来の趣旨は、第２世代の複製を禁止することにより、業としての大量の複製が行われてしまうのを防止することにあり、現在、一般化している「個人使用の範囲内での複製は自由」という著作権についての概念を否定するものではない。

ところで、最近は、ＭＤ（ミニディスク（登録商標））プレーヤや、半導体メモリを内蔵しているカード型メモリプレーヤなどのように、記録再生メディアとして種々のものが登場しており、ユーザも、その日の気分によって、再生メディアとして、ＭＤを用いたり、カード型メモリを用いたりするようになっている。このような現状では複製が頻繁に行われるようになるが、常にオリジナルのメディアからしか複製をすることができないＳＣＭＳ方式では、個人使用の範囲内での複製であるにもかかわらず、不便を来してしまう。

最近のパーソナルコンピュータは、ＣＤプレーヤの機能を備え、ハードディスクにＣＤの音楽情報を格納（複製）して再生できるようになっている。カード型メモリへの複製は、複製速度が速いことから、パーソナルコンピュータのハードディスクからの複製が便利であるが、厳密には、ハードディスクからカード型メモリへの複製は、世代としては第２世代になり、ハードディスクに取り込まれた音楽情報のカード型メモリへの複製はできないことになる。

発明の開示

本発明は、以上の点にかんがみ、ＳＣＭＳ方式を採用することなく、個人使用の範囲での複製は自由にし、かつ、業とした不正な複製を有効に防止することができる方法及び装置を提供することを目的とする。

本発明は、記録媒体の記録及び／又は再生方法であり、データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された使用者識別データと記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、記録媒体から読み出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、記録媒体に記録又は再生を行う。

本発明に係る記録媒体の記録装置は、データとともに使用者を特定するための使用者識別データが記録された記録媒体を走査するヘッド部と、使用者識別データが記憶されたメモリと、ヘッド部によって記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、その比較結果に基づいて記録媒体の記録動作を制御する制御部とを備えている。

また、本発明に係る記録媒体の再生装置は、暗号化処理が施されたデータとともに少なくとも使用者を特定するための使用者識別データと再生管理データが記録された記録媒体を走査するヘッド部と、使用者識別データが記憶されたメモリと、ヘッド部によって記録媒体から読み出された使用者識別データとメモリから読み出された使用者識別データとを比較し、その比較結果に基づいて記録媒体の再生動作を制御する制御部とを備えている。

さたに、本発明は、データの複製制御方法であり、使用者を特定するための使用者識別データが少なくとも埋めこまれたデータから読み出された上記使用者識別データと上記データの複製動作を行う際に装置から読み出された使用者識別データとを比較し、データから抽出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、データの出力制御を行う。

本発明に係るデータの再生方法は、少なくとも使用者を特定するための使用者識別データが埋めこまれたデータから抽出された使用者識別データとデータの再生時に装置から読み出された使用者識別データを比較し、データから抽出された使用者識別データと装置から読み出された使用者識別データとが一致したときに、データの再生を行う。

本発明の更に他の目的、本発明によって得られる具体的な利点は、以下に説明される実施例の説明から一層明らかにされるであろう。

図面の簡単な説明

図１は、ＳＣＭＳ方式による複製世代制限方法を説明するための図である。

図２は、本発明の第１の実施の形態を示すブロック図である。

図３は、本発明の第１の実施の形態の動作説明のためのフローチャートである。

図４は、本発明の第１の実施の形態の動作説明のためのフローチャートである。

図５は、本発明の第１の実施の形態の動作説明のためのフローチャートである。

図６は、本発明の第１の実施の形態における記録処理の説明のためのフローチャートの一部である。

図７は、本発明の第１の実施の形態における記録処理の説明のためのフローチャートの一部である。

図８は、本発明の第１の実施の形態における再生処理の説明のためのフローチャートの一部である。

図９は、本発明の第１の実施の形態における再生処理の説明のためのフローチャートの一部である。

図１０は、本発明の第２の実施の形態のブロック図である。

図１１は、本発明の実施の形態における課金処理システムの全体の概要を説明するための図である。

図１２は、本発明の実施の形態における記録時（複製時）の課金処理を説明するためのフローチャートである。

図１３は、本発明の実施の形態における再生時の課金処理を説明するためのフローチャートである。

発明を実施するための最良の形態

以下、本発明に係るデータ記録再生方法及び装置の具体的な例をディスク記録媒体にオーディオ信号を記録し、再生する場合を例にとって、図面を参照しながら説明する。

図２は、本発明に係るデータ記録再生装置の第１の実施の形態を適用した記録再生システムを示すブロック図である。

図２に示す記録再生システムは、図２に示すように、本発明に係るデータ記録再生装置１０と、使用者識別情報提供装置２０とからなる。使用者識別情報提供装置２０は、以下の説明においては、ユーザＩＤモジュールと称する。この実施の形態においては、データ記録再生装置１０には、ユーザＩＤモジュール２０を

接続するための端子が、必ず設けられている。この接続端子を通じて、データ記録再生装置１０とユーザＩＤモジュール２０との間でやり取りする情報は、安全のため暗号化される。

データ記録再生装置１０は、記録再生用信号処理部（以下、記録再生エンジンチップと称する。）１１と、記録／再生装置部１２と、システム制御部１３と、不揮発性メモリ１４と、入力操作部１５と、表示部１６とを備えている。記録再生エンジンチップ１１は、機能的には、記録エンコード／再生デコード処理部１１１と、ユーザＩＤモジュール２０との間で、暗号化を伴う通信バスを確立して通信を行うための暗号処理部１１２と、制御部１１３とを備えている。

記録再生エンジンチップ１１の記録エンコード／再生デコード処理部１１１は、システム制御部１３の制御を受けて、記録時には、これに対して入力されるアナログオーディオ信号あるいはデジタルオーディオ信号を、後述のように記録エンコード処理して、記録／再生装置部１２に出力し、再生時には、記録／再生装置部１２からの再生データを後述のように再生デコードして、アナログオーディオ信号あるいはデジタルオーディオ信号として出力する。

記録再生エンジンチップ１１の暗号化処理部１１２は、ユーザＩＤモジュール２０に対して、図２に示す例では、ケーブル４０を通じて接続される。この場合、暗号化処理部１１２は、システム制御部１３の制御の下、ユーザＩＤモジュール２０との間で認証作業を行う認証機能を備え、認証がとれたときに、ユーザＩＤモジュール２０との間に通信路を確立する。この場合に、正規の装置1.0であるように見せかける「なりすまし」等の不正行為を防止するため、装置１０とモジュール２０との間で通信を行う前に、装置１０とモジュール２０との間で暗号化及び暗号解除のための新しい暗号鍵の伝達を行い、この新しい暗号鍵を用いて装置１０とモジュール２０との間で通信されるデータを暗号化する。

記録再生エンジンチップ１１の制御部１１３は、システム制御部１３からの制御信号に応じて記録エンコード／再生デコード処理部１１１と、暗号処理部１１２を動作制御すると共に、この制御部１１３に対して接続される不揮発性メモリ１４に対する使用者識別情報の、書き込み、読み出しを制御する。

記録／再生装置部１２は、システム制御部１３による制御を受けて、記録再生

エンジンチップ１１からの記録信号を、ディスク３０に記録し、また、ディスク３０から読み出したデータを、記録再生エンジンチップ１１に供給する。

システム制御部１３は、入力操作部１５を通じた使用者の入力指示に従った制御を行い、また、必要な表示用データを表示部１６に送って、表示部１６の画面に表示する。表示部１６の表示素子としては、液晶ディスプレイなどが用いられる。

ユーザＩＤモジュール２０は、一つのデータ記録再生装置１０に、一つ付属するもので、使用者識別情報（以下、ユーザＩＤという）をデータ記録再生装置１０に供給するものである。ユーザＩＤモジュール２０は、暗号処理及び制御部（以下、セキュアチップと称する）２１と、不揮発性メモリ２２と、入力操作部２３と、表示部２４とを備えている。

セキュアチップ２１は、記録再生エンジンチップ１１との間で認証作業を行う機能を備え、認証がとれたときに、記録再生エンジンチップ１１との間に通信路を確立する。この際に、上述した「なりすまし」等の不正行為を防止するため、装置１０とモジュール２０との間で通信を行う前に、装置１０とモジュール２０との間で暗号化及び暗号解除のための新しい暗号鍵の伝達を行う。

不揮発性メモリ２２には、予め工場出荷時に、各ユーザＩＤモジュール２０に固有のモジュール識別情報（以下、モジュールＩＤと称する）、例えば固有の数値が書き込まれている。

使用者は、データ記録再生装置１０を購入したときに、それに付属しているユーザＩＤモジュール２０に、入力操作部２３を通じて、表示部２４の画面で確認しながら、「ユーザ名」を入力して登録する。

［ユーザＩＤモジュール２０へのユーザ名の登録］

図３は、このユーザＩＤモジュール２０への「ユーザ名」の登録のための処理手順を示すフローチャートである。

先ず、ユーザＩＤモジュール２０は、「ユーザ名」の入力するための画面を、表示部２４に表示し、使用者に、ユーザＩＤモジュール２０への「ユーザ名」の入力を促す（ステップＳ１）。表示部２４の表示に基づいて、使用者が、入力操作部２３を用いてユーザ名を入力すると、ユーザＩＤモジュール２０は、入力操

作部２３によるユーザ名の入力完了を確認した後（ステップＳ２）、入力された「ユーザ名」を、不揮発性メモリ２２に格納する。以上の処理は、セキュアチップ２１が実行するものである。

なお、以上のようにして入力されて登録されたユーザ名は、入力操作部２３を通じた登録ユーザ名の確認操作が行われたときに、不揮発性メモリ２２から読み出されて、表示部２４の画面に表示されて、確認することができるようにされている。

こうして、入力された「ユーザ名」と、不揮発性メモリ２２に予め記憶されていた「モジュールＩＤ」とが、１対１に対応付けられることにより、実質的にモジュールＩＤがユーザＩＤとしての意味を有することになる。つまり、ユーザＩＤは、本発明においては、モジュールＩＤとユーザ名との両方を含む概念を意味する場合と、モジュールＩＤのみからなる概念を意味する場合の２通りの場合がある。

［データ記録再生装置へのユーザＩＤの登録］

以上のようにして、ユーザ名がユーザＩＤモジュール２０に登録された後には、使用者は、ユーザＩＤモジュール２０をデータ記録再生装置１０に接続して、データ記録再生装置１０に対するユーザＩＤ登録を行う必要がある。

図４及び図５は、ユーザＩＤモジュール２０を用いて、データ記録再生装置１０にユーザＩＤの登録をする処理手順を示すフローチャートである。図４は、このときの、ユーザＩＤモジュール２０側での処理であり、また、図５は、データ記録再生装置１０側での処理である。

＜ユーザＩＤモジュール２０側の処理動作＞

ユーザＩＤモジュール２０では、図４に示すように、先ず、データ記録再生装置１０に接続されたかどうか判別する（ステップＳ１１）。ステップＳ１１で接続されていないと判別されたときには、データ記録再生装置１０が接続されていないことを使用者に表示された一覧表４に表示するなどして告知して、使用者に装置１０の接続を促すようにする（ステップＳ１２）。

データ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、使用者による入力操作部２３を通じた「登録指示」を待ち

（ステップＳ１３）、登録指示が受け付けられたことを検知したときには、データ記録再生装置１０の記録再生エンジンチップ１１との間での認証確認すると共に、暗号鍵の伝達を行う（ステップＳ１４）。

記録再生エンジンチップ１１との間で認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ１５）、認証ができずに、通信路が確立できなかったときには、表示部２４にエラー表示をして（ステップＳ１７）、この処理ルーチンを終了する。ステップＳ１５で通信路が確立できたときには、不揮発性メモリ２２からモジュールＩＤ及びユーザ名を読み出し、暗号化して、データ記録再生装置１０に対して、登録命令と共に送信する（ステップＳ１６）。

＜データ記録再生装置１０側の処理動作＞

一方、データ記録再生装置１０側においては、図５に示すように、先ず、ユーザＩＤモジュール２０が接続されるのを待ち、モジュール２０が接続されたことを判別すると（ステップＳ２１）、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０の間での認証確認すると共に、暗号鍵の伝達を行う（ステップＳ２２）。

認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ２３）、ステップＳ２３で認証ができずに、通信路が確立できなかったときには、表示部１６にエラー表示をして（ステップＳ２６）、この処理ルーチンを終了する。

ステップＳ２３で通信路が確立できた判別されたときには、ユーザＩＤモジュール２０からの「モジュールＩＤ」及び「ユーザ名」を含む登録命令の受信を待ち（ステップＳ２４）、受信を確認したら、記録再生エンジンチップ１１は、不揮発性メモリ１４に、受信したモジュールＩＤ及びユーザ名を格納して、所有者登録をする（ステップＳ２５）。

なお、以上のようにして入力されて登録されたユーザ名は、入力操作部１５を通じた登録ユーザ名の確認操作が行われたときに、不揮発性メモリ１４から読み出されて、表示部１６の画面に表示されて、確認することができるようにされている。

データ記録再生装置１０のユーザＩＤは、一旦登録されたものであっても、ユーザＩＤモジュール２０を用いて再登録することにより、別のユーザＩＤに設定

し直すこともできる。

［データ記録再生装置１０での録音処理動作］

次に、データ記録再生装置１０での録音処理動作を図６及び図７に示すフローチャートを参照しながら説明する。

この実施の形態においては、録音をする際には、データ記録再生装置１０には、ユーザＩＤモジュール２０を接続しておく必要がある。すなわち、データ記再生装置１０は、先ず、ユーザＩＤモジュール２０が接続されているかどうか判別する（ステップＳ３１）。ステップＳ３１でユーザＩＤモジュール２０が接続されていないと判別されたときには、ユーザＩＤモジュール２０が接続されていないことを表示部１６に表示するなどして使用者に告知して、モジュール２０の接続を促すようにする（ステップＳ３２）。例えば「ユーザＩＤモジュールが接続されていないので記録はできません。ユーザＩＤモジュールを接続して下さい。」というメッセージを表示部１６に表示したり、音声によるメッセージとして放音することによって使用者に告知する。

ステップＳ３１でデータ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、使用者による入力操作部15を通じた「録音指示」を待ち（ステップＳ３３）、ステップS33で「録音指示」が受け付けられたことを検知したきには、データ記録再生装置１０のシステム制御部１３は、録音命令を記録再生エンジンチップ１１や記録／再生装置部１２に供給し、録音開始準備状態とする（ステップＳ３４）。

次に、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０のセキュアチップ２１との間での認証確認すると共に、暗号鍵の伝達を行う（ステップＳ３５）。認証確認がとれて、通信路が確立できたか否か判別し（ステップＳ３６）、ステップＳ３６で認証ができずに、通信路が確立できなかったときには、録音動作を中止し（ステップＳ３７）、その後、表示部２４にエラー表示をして（ステップＳ３８）、この処理ルーチンを終了する。

ステップＳ３６で、通信路が確立できたと判別したときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０に対して、ユーザＩＤ、つまり、この例の場合には、モジュールＩＤ及びユーザ名の送信要求を出す（ステップＳ３

9）。

ユーザＩＤモジュール２０のセキュアチップ２１は、ユーザＩＤの送信要求に対して、不揮発性メモリ２２からモジュールＩＤ及びユーザ名を読み出し、暗号化して、データ記録再生装置１０に対して送信する。データ記録再生装置１０の記録再生エンジンチップ１１は、このモジュールＩＤ及びユーザ名の受信したか否かをを確認する（ステップＳ４０）。

次に、ステップＳ３１で０で受信を確認した後は、オーディオデータ中に埋め込まれているモジュールＩＤの検出を行い（ステップＳ４１）、モジュールＩＤが検出できたか否か判別する（ステップＳ４２）。ステップＳ４２でモジュールＩＤが検出できたときには、検出されたモジュールＩＤと、ユーザＩＤモジュール２０から取得したモジュールＩＤとを比較照合する（ステップＳ４３）。

ステップＳ４３でのその比較照合の結果、両モジュールＩＤが一致したか否か判別し（ステップＳ４４）、両モジュールＩＤが一致したときには、記録許可となり、入力オーディオデータに圧縮処理を施し、受信したユーザＩＤを暗号鍵とした暗号化処理する（ステップＳ４５）。

この場合、暗号鍵としては、ユーザ名のみを用いる場合、モジュールＩＤのみを用いる場合、又はユーザ名及びモジュールＩＤの両者を用いる場合のいずれであってもよい。

ステップＳ４５で圧縮及び暗号化処理したオーディオデータ中に、ユーザＩＤモジュール２０から取得した「ユーザ名」と、「モジュールＩＤ」とを埋め込む（ステップＳ４６）。この場合に、モジュールＩＤは暗号化して埋め込む。モジュールＩＤを暗号化して埋め込むのはユーザＩＤの秘匿性を高めるためである。ステップＳ４６では、さらに、後述する記録ルールや再生ルールを、記録対象のオーディオデータに埋め込む。

以上のようにして、暗号化し、ユーザＩＤなどを埋め込んだオーディオデータは、記録媒体としてのディスク３０に記録する（ステップＳ４７）。

一方、ステップＳ４２でモジュールＩＤが検出できなかったときと、ステップＳ４４でオーディオデータから検出されたモジュールＩＤとユーザＩＤモジュール２０からのモジュールＩＤとが不一致であったときには、オーディオデータ中

に埋め込まれている記録条件（記録ルール）を検出し（ステップＳ４８）、その検出した記録ルールにしたがった処理を行う（ステップＳ４９）。

この記録ルールの情報の埋め込み処理としては、電子透かし処理と呼ばれている処理や、その他の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、ＴＯＣ（Ｔａｂｌｅ　Ｏｆ　Ｃｏｎｔｅｎｔｓ）データが記録されているエリアなどのオーディオデータが記録されている記録エリアとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

このとき埋め込む記録ルールとしては、例えば、

Ｒ１「無料で記録（複製）可能」

Ｒ２「記録（複製）は有料」

Ｒ３「記録（複製）はフリー」

Ｒ４「記録（複製）は不可」

のうちの一つが選択されて記録されているものである。記録ルールの記録情報としては、記録ルールの内容そのものを記録してもよいが、上述のＲ１～Ｒ４のいずれであるかの情報を記録することもできる。

ここで、Ｒ１「無料で記録（複製）可能」は、ユーザＩＤをオーディオデータに埋め込んで、記録を実行させるものである。これは、この例では、オーサリング装置でレコード会社などにより制作される読み出し専用形式（以下、ＲＯＭタイプという）のディスクなどの記録媒体には、所有者無しとしてユーザＩＤを埋め込まずに記録するので、このＲＯＭタイプの記録媒体からのオーディオデータの記録（複製）時の処理となる。

上記Ｒ２「記録（複製）は有料」は、課金処理が可能な記録装置において、課金処理が実行できたときに記録を許可するものである。課金処理が不能の記録装置の場合には、記録は不可とされる。なお、課金処理の例については、後述する。

上記Ｒ３「記録（複製）はフリー」は、ユーザＩＤはオーディオデータに記録せずに、記録（複製）を行う処理である。さらに、Ｒ４「記録（複製）は不可」は、全く記録（複製）は不可であることを意味している。

上述のように、記録ルールは、ユーザＩＤが不一致の場合だけでなく、記録対象のオーディオデータからユーザＩＤが検出できなかったときにも適用されるが、

ユーザＩＤが不一致の場合と、有効なユーザＩＤが得られない場合とでは、異なる記録ルールを記録しておくようにしてもよい。

また、後述するように、この実施の形態では、再生時には、オーディオデータ中に埋め込まれたユーザＩＤと、不揮発性メモリ１４に格納されたユーザＩＤとの照合を行い、両者が一致したときに、そのオーディオデータの再生が可能となる。この実施の形態では、再生時にオーディオデータからユーザＩＤが検出できなかったとき、また、再生時での照合の結果、ユーザＩＤが不一致であるときに、どのように処理するかの再生ルール（再生条件）も、ステップＳ４６で、オーディオデータ中に埋め込むようにする。

この再生ルールの情報の埋め込み処理としては、記録ルールと同様に、電子透かし処理と呼ばれている処理や、その他の周知の埋め込み処理を用いることができる。また、オーディオデータ中に埋め込むのではなく、ＴＯＣ（Ｔａｂｌｅ Ｏｆ Ｃｏｎｔｅｎｔｓ）データなどのオーディオデータが記録されている記録エリアとは別の記録エリアや、サブコードのエリアなどに記録するようにしてもよい。

この再生時にユーザＩＤが不一致の場合の再生ルールとしては、例えば、

ＰＢ１「無料再生可能」

ＰＢ２「再生禁止（再生不可）」

ＰＢ３「再生は有料」

ＰＢ４「制限付きで再生可能」

のうちの一つが選択されて記録されるものである。再生ルールの記録情報としては、再生ルールの内容そのものを記録してもよいが、上述のＰＢ１～ＰＢ４のいずれであるかの情報を記録することもできる。

ここで、上記ＰＢ１「無料再生可能」の場合には、再生装置に登録されたユーザＩＤに関係なく、常に、オーディオデータの再生可能となり、ＰＢ２「再生禁止（再生不可）」の場合には、再生装置に登録されたユーザＩＤと不一致の場合、常に、オーディオデータの再生が禁止される。前述したように、この例では、オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体には、ユーザＩＤを埋め込まずに記録するので、再生オーディオデ

ータから有効なユーザＩＤが得られない場合として、上記ＰＢ①のルールが記録される。

また、上記ＰＢ３「再生は有料」の場合には、課金処理が可能な再生装置において、課金処理が実行できたときに、オーディオデータの再生を許可するものである。課金処理が不能の再生装置の場合には、オーディオデータの再生は不可とされる。なお、課金処理の例については、後述する。

上記ＰＢ４「制限付きで再生可能」は、例えば、全部又は一部の試聴モードを許可し、その試聴モードの後は、上記ＰＢ２又はＰＢ３のルールとするものである。ここで、試聴モードとは、

ａ）ｎ回、例えば１回だけ無料再生可能

ｂ）ｍ秒分だけ無料再生可能

ｃ）さわり部分やさび部分だけ無料再生可能

を意味する。

このＰＢ４「制限付き再生可能」の再生ルールで、前記ａ）やｂ）を採用する場合には、再生装置は、例えば、ＩＳＲＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｔａｎｄａｒｄ Ｒｅｃｏｒｄｉｎｇ Ｃｏｄｅ）などのコンテンツＩＤ（識別コード）に対応させて、そのコンテンツＩＤで識別されるオーディオデータの試聴履歴の情報、例えば試聴回数や、試聴秒数などを記録するようにする。

この実施の形態では、後述の再生処理で説明するように、この再生ルールは、再生時にユーザＩＤが不一致の場合だけでなく、再生オーディオデータから、有効なユーザＩＤが得られないときにも共通に適用される。しかし、ユーザＩＤが不一致の場合と、有効なユーザＩＤが得られない場合とでは、異なる再生ルールを記録するようにしてもよい。

例えば、オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体にも、ユーザＩＤとして、例えば「ＯＲＩＧＩＮＡＬ」などの特定のＩＤ、すなわち、記録媒体がオリジナルであることを示す識別データが記録される場合には、再生装置は、その特定のＩＤを検出したときには、自己の装置のユーザＩＤと不一致の場合でも、再生許可すべきである。したがって、再生ルールが埋め込まれるものとした場合には、その再生ルールは、「再生

可能」とされる。

一方、このように特定のユーザＩＤが、ＲＯＭタイプのディスクなどの記録媒体の記録データに埋め込まれるなどして、記録データに付随して記録されると定められている場合には、再生装置において、有効なユーザＩＤが得られないときには、そのオーディオデータは、不正に記録されたものであるとすることができる。したがって、その時の再生ルールは再生不可とするのがよい。

オーサリング装置でレコード会社などにより制作されるＲＯＭタイプのディスクなどの記録媒体には、ユーザＩＤを記録しないと定められている場合には、上述のような再生ルールのうちの一つを共通に用いることができる。

[データ記録再生装置１０での再生処理動作]

次に、以上のようにして録音されたオーディオデータを、データ記録再生装置１０で再生する場合の処理動作を図８及び図９のフローチャートを参照しながら説明する。

先ず、記録済みのディスクが装填されるのを待ち、装填されたことを判別すると（ステップＳ５１）、記録再生エンジンチップ１１は、使用者からの再生指示を待つ。そして、使用者からの入力操作部１５による再生指示を確認すると（ステップＳ５２）、ディスクから再生指示のあったオーディオデータを読み出す（ステップＳ５３）。

読み出されたオーディオデータに埋め込まれているユーザＩＤを検出する。ユーザＩＤのうちの、この例では、暗号化されているモジュールＩＤの暗号を解除して検出する（ステップＳ５４）。モジュールＩＤが検出できたか否か判別し（ステップＳ５５）、検出できなかったときには、再生オーディオデータに埋め込まれている再生ルールを検出し（ステップＳ７３）、その検出された再生ルールに従った処理を行う（ステップＳ７４）。

ステップＳ５５で、モジュールＩＤを検出することができたと判別されたときには、その検出されたモジュールＩＤと、不揮発性メモリ１４に記憶されているモジュールＩＤとを比較照合する（ステップＳ５６）。

両モジュールＩＤが一致しているかどうか判別し（ステップＳ５７）、ステップＳ５７で両モジュールＩＤが一致しているときには、ユーザＩＤが用いられて

暗号化されているオーディオデータの暗号を解き（ステップＳ５８）、オーディオデータの圧縮を解凍、即ち、伸張処理する（ステップＳ５９）。伸張されたオーディオデータを復号して、再生出力する（ステップＳ６０）。

一方、ステップＳ５７で、ディスク３０から読み出したデータから検出されたモジュールＩＤと、不揮発性メモリ１４から読み出されたモジュールＩＤとが不一致であると判別されたときには、ユーザに、ユーザＩＤモジュール２０を接続させる設定になっているかどうかを判別し、その判別の結果、ユーザＩＤモジュールを接続させる設定になっていなければ、再生オーディオデータに埋め込まれている再生ルールを検出し（ステップＳ７３）、その検出された再生ルールに従った処理を行う（ステップＳ７４）。この例では、例えばディスク３０の再生が禁止となる。

この場合の再生禁止には、装置１０が正常な再生出力が行われないことも含まれる。つまり、装置１０からの再生出力としてノイズが出力される場合の他、装置１０からの再生出力に代えて、「違法に複製された記録媒体からの再生である」旨のメッセージを、オーディオ出力として装置１０から送出するようにしてもよい。

ステップＳ６１で、ユーザに、ユーザＩＤモジュールを接続させる設定になっていると判別されたときには、データ記録再生装置１０は、ユーザＩＤモジュール２０が接続されているかどうか判別する（ステップＳ６２）。ステップＳ６２で接続されていないと判別されたときには、ユーザＩＤモジュール２０が接続されていないことを使用者に報知して、モジュール２０の接続を促すようにする（ステップＳ６３）。

データ記録再生装置１０にユーザＩＤモジュール２０が接続されていることが検知されたときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０との間での認証確認すると共に、暗号鍵の伝達を行う（ステップＳ６４）。認証確認がとれて、チップ１１とモジュール２０との間で通信路が確立できたか否か判別し（ステップＳ６５）、認証ができずに、チップ１１とモジュール２０との間で通信路が確立できなかったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行う（ステップＳ７３、ステップＳ７４）。この例では、

前述のようにディスク３０の再生が禁止となる。

ステップＳ６５で、チップ１１とモジュール２０との間で通信路が確立できたと判別したときには、記録再生エンジンチップ１１は、ユーザＩＤモジュール２０に対して、ユーザＩＤのうちの、この例の場合には、モジュールＩＤの送信要求を出す（ステップＳ６６）。

ユーザＩＤモジュール２０のセキュアチップ２１は、エンジンチップ１１からのこの送信要求に対して、不揮発性メモリ２２からモジュールＩＤを読み出し、暗号化して、データ記録再生装置１０に対して送信する。データ記録再生装置１０の記録再生エンジンチップ１１は、ユーザＩＤモジュール２０から送信されてきたモジュールＩＤの受信を確認すると（ステップＳ６７）、ディスク３０から読み出したデータから検出されたモジュールＩＤと、受信し暗号を解いた又は復号したモジュールＩＤとを比較照合する（ステップＳ６８）。

両モジュールＩＤが一致しているかどうか判別し（ステップＳ６９）、両モジュールＩＤが不一致であったときには、オーディオデータに埋め込まれた再生ルールに従った処理を行う（ステップＳ７３、ステップＳ７４）。前述したように、この例では、ディスク３０の再生禁止となる。

両モジュールＩＤが一致したときには、ユーザＩＤが用いられて暗号化されているオーディオデータの暗号を解き、即ち復号し（ステップＳ７０）、オーディオデータの圧縮を解凍、即ち伸張処理する（ステップＳ７１）。圧縮が解凍された、即ち伸張処理されたオーディオデータを復号して、再生出力する（ステップＳ７２）。

以上のようにして、この実施の形態においては、記録時に、登録されたユーザＩＤを記録データに埋め込んで記録し、再生時には、不揮発性メモリ１４に登録されたユーザＩＤと、ディスク３０から読み出されたデータから検出されたユーザＩＤとを比較して、両ユーザＩＤが一致したときに、ディスクから読み出されたデータの正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

上述の実施の形態では、記録時には、ユーザＩＤモジュール２０を、データ記録再生装置１０に接続した状態ではないと記録を実行することができないように

したので、この点でも、ユーザの個人使用の範囲内での制限をすることができる。

この実施の形態では、記録側に上記のような制限を加えた代わりに、再生側においては、不揮発性メモリ１４に登録されたユーザＩＤと、ディスク３０から読み出されたデータから検出されたユーザＩＤとを比較して、両ユーザＩＤが一致しているかどうかを判別するようにしており、記録時のように、ユーザＩＤモジュール２０を接続する必要はなく、再生時におけるユーザの使い勝手が良くなるという効果がある。

例えば、「個人使用の範囲でコピーは自由」ということを具現化する方法として、個人で取得済みの聴取権情報（例えば、その個人が持っているコンテンツの全ての情報）を自分専用のＩＣカードに記録しておき、コンテンツを再生する際には、必ずそのＩＣカードを再生装置に差し込むようにする方法が考えられる。この場合、ＩＣカードを他人が使えない状態に保つために、一人一枚のＩＣカードを持つように管理される。

このようにすれば、ＩＣカードが、その個人の全ての聴取権情報を持つので、コンテンツの複製は、全く自由にしてしまっても問題がなくなるが、その代わりに、使用者は、再生装置に差し込むＩＣカードを持ち歩かなければならなくなるという問題がある。

上述の実施の形態の場合には、再生装置には、そのＩＣカードのようなものは不要となるので、非常に便利である。

上述の実施の形態では、記録データは、ユーザＩＤを暗号鍵とした暗号を施して記録するようにしているので、再生時には、ユーザＩＤが一致したときにしか、記録データの暗号化が解除、復号できなくなり、より個人使用の範囲内での制限を確実にすることができる。

なお、ユーザＩＤを暗号鍵そのものとせず、記録データの暗号化の鍵を取得するための情報などのように、暗号化に関連する情報として用いても、同様の効果が得られると期待できる。但し、記録ルール又は再生ルールでユーザＩＤが不一致の場合にも記録又は再生を許可している場合には、必ずしもユーザＩＤを暗号鍵に用いなくともよい。

上述の実施の形態では、ユーザＩＤモジュール２０からのユーザＩＤの情報は、

暗号化してデータ記録再生装置１０に送るようにしており、このため、ユーザＩＤの秘匿性を高めることができるという効果もある。

上述の説明では、記録ルール及び再生ルールをオーディオデータに埋め込んだので、記録ルール及び再生ルールの情報は、オーディオデータから検出するようにするが、記録ルール及び再生ルールの情報が、ＴＯＣエリア又ＴＯＣデータ内などに記録されていた場合には、記録対象のオーディオデータの記録又は再生動作に先立ち、記録ルール及び再生ルールの情報を取得するようにすればよい。

オーディオデータが圧縮されてブロック化されている場合には、ブロックとブロックの間の隙間に記録ルール及び再生ルールの情報を埋め込むようにすることもできる。その場合には、圧縮デコードのときに、記録ルール及び再生ルールの情報を抽出することができる。

データ記録再生装置１０が、データの再生と記録が同時にでき、データの複製記録ができるように、記録媒体を同時に複数枚装填できるようにされている場合には、再生側のディスクから記録ルールや再生ルールの情報を予めＴＯＣデータや再生データから得るようにすることもできる。

なお、以上の実施の形態では、記録ルール及び再生ルールをオーディオデータ中に必ず記録するように説明したが、予め、システムとして、ユーザＩＤが得られなかったとき、また、ユーザＩＤが不一致のときの、記録ルール及び再生ルールを、例えば上述のルールのうちの一つに定めておくようにすれば、記録ルール及び再生ルールをオーディオデータ中に記録する必要はなくなる。

［第２の実施の形態］

この第２の実施の形態は、データ記録再生装置が、パーソナルコンピュータに搭載される場合の例である。図１０は、この第２の実施の形態の場合のシステムのブロック図である。

この第２の実施の形態のシステムは、パーソナルコンピュータ５０と、前述の第１の実施の形態の場合に用いたユーザＩＤモジュール２０とにより構成される。

この実施の形態のパーソナルコンピュータ５０は、ユーザＩＤモジュール２０を接続するための端子を備えている。このモジュール２０を接続するための端子を通じて、パーソナルコンピュータ５０とユーザＩＤモジュール２０との間でや

り取りする情報は、全て暗号化されるものである。

パーソナルコンピュータ５０は、第１の実施の形態のデータ記録再生装置１０と同様に、記録再生エンジン５１と、記録／再生装置部５２と、不揮発性メモリ５４とを備えると共に、システムバス５９を介して、ＣＰＵ５３と、入力操作部５５と、表示部５６と、ネットワークインターフェース５７と、ハードディスク装置５８とが接続される。システムバス５９には、記録再生エンジン５１と、記録及び／又は再生装置部５２も接続されている。

ネットワークインターフェース５７は、ネットワーク６０に接続された記憶装置６１に対して接続される。ここで、ネットワーク６０は、ローカルエリアネットワーク（ＬＡＮ）であっても良いし、インターネットであってもよい。インターネットの場合には、記憶装置６１は、所定のサーバなどに設けられた記録装置とされる。

この第２の実施の形態においても、前述の第１の実施の形態と全く同様にして、ユーザＩＤモジュール２０には、ユーザ名が入力登録され、その後、パーソナルコンピュータ５０にユーザＩＤの登録処理が、ユーザＩＤモジュール２０から、パーソナルコンピュータ５０に対して行われて、不揮発性メモリ５４には、ユーザＩＤが登録されて記憶される。

この第２の実施の形態の場合には、記録メディアとしては、第１の実施の形態の場合のディスク３０のみではなく、ハードディスク装置５８やネットワーク６０に接続された記憶装置１６も用いられる。

すなわち、この第２の実施の形態の場合の記録における入力ソースと、記録媒体（記録メディア）との組み合わせを示すと、

１．アナログ入力あるいはデジタル入力→ディスク３０

２．アナログ入力あるいはデジタル入力→ハードディスク装置５８

３．アナログ入力あるいはデジタル入力→記憶装置６１

４．ディスク３０→ハードディスク装置５８

５．ディスク３０→記憶装置６１

６．ハードディスク装置５８→ディスク３０

７．ハードディスク装置５８→記憶装置６１

８．記憶装置６１→ディスク３０

９．記憶装置６１→ハードディスク装置５８

などがある。

これら９通りの他にも、ネットワーク６０上の一つの記憶装置から、他の記憶装置に転送して書き込む処理も、記録処理の一つと考えられる。以上のいずれの記録時においても、この第２の実施の形態では、前述の第１の実施の形態と同様にして、ユーザＩＤモジュール２０が接続されることを条件とすると共に、そのユーザＩＤモジュール２０から取得したユーザ名及びモジュールＩＤとを、記録データに埋め込んで記録するようにする。この場合に、第１の実施の形態と同様に、モジュールＩＤは、暗号化して記録する。

この場合、ハードディスク装置５８への記録の場合には、記録再生エンジンチップ１１で記録エンコードされたデータは、記録／再生装置部５２を経ることなく、システムバス５９を通じてハードディスク装置５８に送られて、ハードディスクに格納される。

記憶装置６１への記録の場合には、記録再生エンジンチップ１１で記録エンコードされたデータは、記録／再生装置部５２を経ることなく、システムバス５９及びネットワークインターフェース５７を通じて記憶装置６１に対してネットワーク６０に送出され、記憶装置６１に格納されるようにされる。

ディスク３０、ハードディスク装置５８、記憶装置６２のいずれからのオーディオデータの再生時においても、前述の第１の実施の形態と全く同様に、再生データ中から検出したユーザＩＤと、不揮発性メモリ５４に記憶されていたユーザＩＤとの照合が行われて、両者が一致したときに、オーディオデータの再生出力を可能とするようにする。

この第２の実施の形態の場合にも、上述した第１の実施の形態と同様の効果が得られると共に、ハードディスク装置５８を用いた高速複製が、ユーザの個人使用の範囲内という制限を保持して可能となる。ネットワークを通じた記憶装置へのデータ転送も、一つの記録（複製）態様とすることができるが、それも、ユーザの個人使用の範囲内という制限を保持して可能となる。

［課金処理の例について］

次に、記録ルール及び再生ルールが課金を条件にしている場合に対応する実施の形態を説明する。図１１は、この例の課金処理システムの一例を示すものであり、音楽コンテンツの配付、音楽コンテンツのデータの授受については、省略されている。この実施の形態のデータ記録再生装置１０は、複製記録ができるように構成されている。つまり、あるディスクからのデータを、別のディスクに記録することが可能とされている。

この実施の形態の場合、課金処理のために、記録に際しては複製権データが、再生に際しては聴取権データが、それぞれ使用される。これら複製権データおよび聴取権データは、ＩＣカードや、データ記録再生装置１０に設けられるセキュアデコーダ１７のメモリに格納される。

複製権データ及び聴取権データは、例えば複製可能な度数及び再生可能な度数であり、データ記録再生装置１０が課金対象のコンテンツを記録／再生する度に、それぞれの度数が減算される。

これら複製権データ及び聴取権データは、複製／聴取権データ管理会社の管理下で、ユーザが所有する複製／聴取権データチャージャ又は販売店に設置された複製／聴取権データ販売端末２０５によって書き替えることが可能とされている。この例では、複製／聴取権データチャージャは、ユーザＩＤモジュール２０内に課金データチャージャ２５として設けられている。

課金データチャージャ２５は、データ記録再生装置１０のセキュアデコーダ１７と決済センター２０３又はレコード店、コンビニエンスストア等に設置されているデータ販売端末２０５との間に存在して聴取権データ中継器として機能する。

レコード会社２０１、著作権管理機構２０２、ユーザデバイスとしてのデータ記録再生装置１０と関係して、代金決済のために、決済センター２０３が存在している。決済センター２０３は、認証／課金サーバを備えている。決済センター２０３は、銀行、クレジットカード会社２０４との間で代金の決済を行う。

図１１において、破線で示すように、レコード会社２０１から配布される、記録再生装置１０が再生する媒体（光ディスク、メモリカード等）には、音楽コンテンツが記録されている。音楽コンテンツの配信の方法は、この他、種々のものが使用できる。また、記録再生装置１０は音楽コンテンツを媒体（光ディスク、

メモリカード等）３０に記録する。

データ記録再生装置１０内のセキュアデコーダ１７と、課金データチャージャ２５とが、この例では有線の通信路を介して通信を行い、複製／聴取権データが課金データチャージャ２５からセキユアデコーダ１７内のメモリに対して転送される。複製／聴取権データは、例えばデータ記録再生装置１０の、記録（複製）可能回数又は記録（複製）可能時間／再生可能回数情報又は再生可能時間に対応している。

データ記録再生装置１０のセキュアデコーダ１７から課金データチャージャ２５に対して、データ記録再生装置１０の複製／再生履歴情報（複製／再生ログ）が伝送される。複製ログには、複製したデータの識別子及び／又は又は複製の条件を含む。具体的には、複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報を含んでいる。

再生ログは、復号したディジタルデータの識別子及び／又は復号の条件を含む。具体的には、聴取した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報を含んでいる。この例では、再生時には、復号に対して課金される。

複製／再生ログには、ユーザ端末の所有者、ユーザデバイスとしてのデータ記録再生装置１０の識別子等の課金対象者を特定するための識別子が含まれている。セキュアデコーダ１７と課金データチャージャ２５との間では、前述の図２に示した暗号処理部１１２と暗号処理及び制御部２１を利用して、必要に応じて認証を行い、暗号処理部１１２と制御部２１との間で認証が成立すると、暗号化された複製／聴取権データ及び複製／再生ログの伝送がなされる。

複製／聴取権データは、決済センター２０３から通信路２０６例えば電話回線を介して課金データチャージャ２５に渡される。又は、決済センター２０３から通信路２０７を介して販売端末２０５に渡された複製／聴取権データが通信路２０８を介して課金データチャージャ２５に渡される。この場合にも、セキュリティの確保のために、例えば決済センター２０３と課金データチャージ２５との間で認証と暗号化とがなされる。

課金データチャージャ２５に吸い上げられた複製／再生ログは、通信路２０６を介して決済センター２０３に送られる。又は、複製／再生ログは、通信路２０

８を介して販売端末２０５に渡される。販売端末２０５は、通信路２０７を介して決済センター２０３から聴取権データを受け取ると共に、再生ログを決済センター２０３へ送る。さらに、販売端末２０５は、入手した聴取権データの代金を決済センター２０３に支払う。通信路２０７は、電話回線、インターネット等である。

決済センター２０３と聴取権データチャージャ２５との間では、通信路２０６を介して複製／聴取権データ及び複製／再生ログの送受信がなされる。この場合にも、セキュリティの確保のために、決済センタ２０３と聴取権データチャージャ２５との間で認証とデータ授受の際の暗号化とがなされる。聴取権データの決済に関して、銀行、クレジットカード会社２０４が存在している。銀行、クレジットカード会社２０４は、予め登録してあるユーザの銀行口座から決済センター２０３の依頼に基づいて、課金データチャージャ２５に書き込んだ複製／聴取権データに相当する金額を引き落とす。

さらに、決済センター２０３は、レコード会社２０１から複製／聴取権データに関するサービスの管理の委託を受ける。決済センター２０３は、レコード会社２０１に対して複製／聴取権データに関する技術の提供を行い、さらに、楽曲聴取料を支払う。レコード会社２０１は、著作権管理機構２０２に対して著作権の登録を行うことによって、著作権の管理を依頼し、著作権管理機構２０２から著作権料を受け取る。

なお、通信路２０８の代わりに、ＩＣカードを利用することもできる。すなわち、課金データチャージャ２５及び販売端末２０５は、ＩＣカードの書込み／読出し部を備えるようにする。ＩＣカードを課金データチャージャ２５に差し込んだ時には、課金データチャージャ２５は、ＩＣカードに格納されている複製／聴取権データを吸い上げるとともに、複製／再生ログのデータをＩＣカードに書き込むようにする。ＩＣカードの複製／聴取権データは、課金データチャージャ２５に吸い上げられると、クリアされて零となる。

販売端末２０５にＩＣカードを差し込んだ時には、ユーザが必要な複製／聴取権データの度数を設定することにより、当該設定された複製／聴取権データがＩＣカードに書き込まれる。このとき、同時に、ＩＣカードに格納されていた複製

／再生ログが販売端末２０５に吸い上げられ、ＩＣカードの複製／再生ログは、クリアされる。

以上説明したような課金システムにおいて、この実施の形態では、記録ルール又は再生ルールとして、課金処理が必要な処理が設定されていた場合には、データ記録再生装置１０のセキュアデコーダ１７において、複製又は再生についての課金処理が実行される。

図１２は、複製記録の際のステップＳ４８において、記録ルールが課金を伴う記録と設定されている場合におけるステップＳ４９での処理のフローチャートである。

すなわち、先ず、セキュアデコーダ１７のメモリの複製権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップＳ８１）。ステップＳ８１で課金処理が可能であると判別されたときには、記録（複製）を実行する（ステップＳ８２）。記録が終了したことを確認すると（ステップＳ８３）、セキュアデコーダ１７のメモリの複製権データの度数を減じる（ステップＳ８４）。そして、複製ログとして、例えば複製した音楽コンテンツの識別子、種類、複製回数、複製時間等の情報をそのメモリに記憶し（ステップＳ８５）、課金処理を終了する。

一方、セキュアデコーダ１７のメモリの複製権データの度数の残が無く、ステップＳ８１で課金処理が不可と判別された場合には、複製権データの度数残が無い旨のメッセージを表示するなどしてユーザに知らせる（ステップＳ８６）。複製権データが追加されたか否か判別し（ステップＳ８７）、追加されたときには、ステップＳ８２に進み、記録を実行して、上述のステップＳ８３以降の処理を行う。ステップＳ８７で複製権データの追加が無かったと判別されたときには、記録不可と判定して（ステップＳ８８）、この課金処理ルーチンを終了する。

図１３は、再生の際のステップＳ７３において、再生ルールが課金を伴う再生と設定されている場合におけるステップＳ７４での処理のフローチャートである。

すなわち、先ず、セキュアデコーダ１７のメモリの聴取権データの度数の残を調べ、課金処理可能であるか否か判別する（ステップＳ９１）。ステップＳ９１で課金処理が可能であると判別されたときには、再生データの暗号を解除する復

号を実行する（ステップＳ９２）。復号が完了したことを確認すると（ステップＳ９３）、セキュアデコーダ１７のメモリの聴取権データの度数を減じる（ステップＳ９４）。再生ログとして、例えば再生した音楽コンテンツの識別子、種類、再生回数、再生時間等の情報をそのメモリに記憶し（ステップＳ９５）、課金処理を終了する。

一方、セキュアデコーダ１７のメモリの聴取権データの度数の残が無く、ステップＳ９１で課金処理が不可と判定された場合には、聴取権データの度数残が無い旨のメッセージを表示するなどしてユーザに知らせる（ステップＳ９６）。聴取権データが追加されたか否か判別し（ステップＳ９７）、ステップＳ９７で追加されたと判定されたときには、ステップＳ９２に進み、復号を実行して、上述のステップＳ９３以降の処理を行う。ステップＳ９７で聴取権データの追加が無かったときには、再生不可として再生動作を禁止し（ステップＳ９８）、この課金処理ルーチンを終了する。

なお、ステップＳ９８では、完全に再生不可とするのではなく、さわりの部分やさびの部分のみの再生を可とするようにしてもよい。

［その他の実施の形態］

上述の実施の形態においては、再生時には、ユーザＩＤモジュールは、データ記録再生装置あるいはパーソナルコンピュータには接続しなくても再生可能としたが、再生時にも、ユーザＩＤモジュールを接続しなければ、再生できないような仕組みとしてもよい。すなわち、不揮発性メモリ１４を設けずに、再生時にもユーザＩＤモジュールの接続を必須として、ユーザＩＤモジュールからのユーザＩＤと、再生データから検出したユーザＩＤとを照合するようにしてもよい。

再生処理としては、上述の実施の形態と同様とするも、例えば、再生前に、データ記録再生装置に対するユーザＩＤモジュールの接続を確認し、不揮発性メモリ１４に記憶されているユーザＩＤと、使用者を示すユーザＩＤモジュールからのユーザＩＤとの照合を行って、使用者を確認してから、上述の再生動作を行うようにすることもできる。

上述の実施の形態の場合においては、記録時には、ユーザＩＤモジュールの証確認は行うが、ユーザＩＤを用いた確認は行っていない。しかし、記録時に、ユ

ーザＩＤモジュールをデータ記録再生装置に接続したときに、ユーザＩＤを用いたユーザＩＤモジュールの認証確認を行うようにしてもよい。

上述の実施の形態は、記録再生装置の場合であるが、記録専用装置や、再生専用装置にも、この発明は適用可能である。その場合、ユーザＩＤモジュールは、上述の第１及び第２の実施の形態と同様の形態では、記録専用装置に付属すべきものである。再生専用装置の場合には、再生専用装置には、ユーザＩＤを、その不揮発性メモリに一旦登録すれば、再生時には、再生装置にユーザＩＤモジュールを接続しておく必要はない。

もっとも、これらの実施の形態にも、上述のその他の実施の形態を適用することも、勿論できる。

なお、上述の第１及び第２の実施の形態におけるユーザＩＤ登録は、データ記録再生装置のうちの再生装置部分に対するユーザ登録である。前述の第１及び第２の実施の形態では、記録装置に対しては、ユーザＩＤモジュールを必ず接続して、そのユーザＩＤを記録するようにするので、記録装置部分のみを考え場合には、ユーザＩＤを登録する必要はない。

しかし、記録専用装置や記録再生装置の記録装置部分の機能を特定の使用者専用とする場合には、ユーザＩＤモジュールを用いて、ユーザＩＤを登録して不揮発性メモリに記憶しておき、記録の際にユーザＩＤが一致したときに、記録が可能となるようにする仕組みとすることもできる。

上述の実施の形態では、ユーザＩＤとしては、ユーザ名やモジュールＩＤを用いるようにしたが、使用者の指紋や声紋、あるいは脈などの各個人に固有の生体情報を使用するようにしても良い。その場合に、再生装置では、不揮発性メモリに記憶されている生体情報のユーザＩＤと再生データから検出した生体情報のユーザＩＤとを照合するようにしても良いが、不揮発性メモリを設けずに、再生データから検出した生体情報のユーザＩＤと、指紋や声紋、あるいは脈などの生体情報入力手段から入力された生体情報のユーザＩＤとを照合するようにすることもできる。この場合に、生体情報入力手段は、ユーザＩＤモジュールを用いることができる。

なお、音楽会社などから提供される読み出し専用形式のディスクのように、市

販される記録媒体は、「オリジナル」として扱うこととし、前述したように、所有者は無しとされる。ただし、この「オリジナル」から複製が行われた場合には、その複製には、前述したように、ユーザＩＤが記録され、所有者が特定されることになる。

上述の実施の形態では、ユーザ名については、特に制限を付けなかったが、ユーザ名は個人名であっても、ファミリー名のようなグループ名であってもよい。要するに、著作権法上「個人の使用の範囲内」と認められるような範囲で共有が可能である。

１台の記録ないし再生装置に、複数個のユーザＩＤを登録することができるようにして、前記１台の装置を、前記複数個のユーザＩＤに対応する複数の使用者で共有するようにすることもできる。

上述の実施の形態では、ユーザＩＤは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザＩＤを記録データに付加することができる。

上述の実施の形態では、記録時には、ユーザＩＤモジュール２０をデータ記録再生装置１０に接続することを必須としたが、記録時に、ユーザＩＤモジュール２０を接続することなく、データ記録再生装置１０の不揮発性メモリ１４に蓄えられているユーザＩＤ（特にモジュールＩＤ）と、記録対象のデータに付随するユーザＩＤとを比較照合するようにしてもよい。

記録ルールとして、不揮発性メモリ１４に記憶されているユーザＩＤと、記録対象のデータに付随するユーザＩＤとが一致したときには、ユーザＩＤモジュール２０はデータ記録再生装置１０には接続不要という設定を行えるようにしてもよい。

記録対象のデータに付随するユーザＩＤというときには、記録対象のデータに埋め込まれていることのみを意味するのではなく、上述もしたように、記録媒体のＴＯＣエリアや、その他の記録対象データの記録部分とは別個のエリアから、ユーザＩＤを取得することも含む。また、インターネットからダウンロードしたデータを記録対象とする場合に、そのダウンロードデータの最初、中間あるいは

最後に、ユーザＩＤが付加されるような場合も含む。

記録対象のデータは、データ記録再生装置１０において記録媒体から再生されたものではなく、アナログ入力とされた、あるいはデジタル入力とされたデータを含むものであることは言うまでもない。その場合に、その入力データは、ディスクから再生された再生データである必要もない。

なお、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

記録媒体としては、ディスクに限らず、カード形メモリや、半導体メモリ、ハードディスク装置のハードディスクなどであってもよい。さらに、記録対象となるデータは、前述もしたように、記録媒体から再生されたデータに限られるものではなく、有線電話回線や無線電話回線又はインターネットを通じて送られてくるデータであってもよい。

また、上述の実施の形態は、記録対象のコンテンツとして、オーディオデータを例にとったが、映像データやプログラム、ゲームのプログラムやデータなど、著作権管理が必要なコンテンツのいずれも、この発明の記録対象である。

上述の実施の形態では、ユーザＩＤは、記録データに埋め込むようにしたが、記録データとは別領域に記録するようにしても勿論よい。また、記録データを、コンピュータデータのようにファイル単位に取り扱う場合には、ファイル単位にユーザＩＤを記録データに付加することができる。

産業上の利用可能性

本発明によれば、記録時に、登録されたユーザＩＤを記録データと共に記録し、再生時には、不揮発性メモリ１４などに用意されるユーザＩＤと、記録媒体から読み出されたデータから検出されたユーザＩＤとを比較して、両者が一致したときに、正常な再生出力を行うようにしたことにより、個人的な利用形態に限って複製を可能にすることができる。

請求の範囲

１．データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の記録又は再生時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体に記録又は再生を行う記録媒体の記録及び／又は再生方法。

２．上記記録媒体には、更に上記記録媒体の記録又は再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体に記録又は再生を行う請求の範囲第１項記載の記録媒体の記録及び／又は再生方法。

３．上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記記録媒体に記録する請求の範囲第１項記載の記録媒体の記録及び／又は再生方法。

４．上記方法は、上記装置から読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第３項記載の記録媒体の記録及び／又は再生方法。

５．上記方法は、上記装置から読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第３項記載の記録媒体の記録及び／又は再生方法。

６．上記記録媒体には、更に上記記録媒体の記録又は再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒

体の再生を行う請求の範囲第１項記載の記録媒体の記録及び／又は再生方法。

７．上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記記録媒体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第６項記載の記録媒体の記録及び／又は再生方法。

８．上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第７項記載の記録媒体の記録及び／又は再生方法。

９．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第１項記載の記録媒体の記録及び／又は再生方法。

１０．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第９項記載の記録媒体の記録及び／又は再生方法。

１１．データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の記録時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体に記録を行う記録媒体の記録方法。

１２．上記記録媒体には、更に上記記録媒体の記録動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の記録を行う請求の範囲第１１項記載の記録媒体の記録方法。

１３．上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記記録媒体に記録する請求の範囲第１１項記載の記録媒体の記録方法。

１４．上記方法は、上記装置から読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第１３項記載の記録媒体の記録方法。

１５．上記方法は、上記装置から読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第１４項記載の記録媒体の記録方法。

１６．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第１１項記載の記録媒体の記録方法。

１７．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第１６項記載の記録媒体の記録方法。

１８．データとともに使用者を特定するための使用者識別データが記録された記録媒体を走査するヘッド部と、

使用者識別データが記憶されたメモリと、

上記ヘッド部によって上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、上記比較結果に基づいて上記記録媒体の記録動作を制御する制御部とを備えている記録媒体の記録装置。

１９．上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記ヘッド部を制御して上記記録媒体に記録を行う請求の範囲第１８項記載の記録媒体の記録装置。

２０．上記メモリは、上記装置に接続される使用者識別データ提供部に設けられている請求の範囲第１８項記載の記録媒体の記録装置。

２１．上記制御部は、上記装置に上記提供部が接続されていると判別されたときには上記提供部との間で認証処理を行う請求の範囲第２０項記載の記録媒体の記録装置。

２２．上記制御部は、上記認証処理が正しく終下したときには上記提供部に上記メモリから上記使用者識別データを読み出すように指示をする請求の範囲第２１項記載の記録媒体の記録装置。

２３．上記メモリから読み出された使用者識別データは暗号化処理が施されて、上記提供部から上記制御部に送信される請求の範囲第２２項記載の記録媒体の記録装置。

２４．上記制御部は、上記認証処理が正しく終了できなかったときには上記記録媒体の記録動作を中止する請求の範囲第２１項記載の記録媒体の記録装置。

２５．上記制御部は、上記装置に上記提供部が接続されていないと判別されたときには使用者に上記提供部を接続するように告知する請求の範囲第２１項記載の記録媒体の記録装置。

２６．上記記録媒体には、更に上記記録媒体の記録動作を管理するための管理データが記録されており、上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の記録を行う請求の範囲第１９項記載の記録媒体の記録装置。

２７．上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記記録媒体に記録するデータに暗号化処理を施して上記ヘッド部により上記記録媒体に記録する請求の範囲第２６項記載の記録媒体の記録装置。

２８．上記制御部は、上記メモリから読み出された使用者識別データを上記記録媒体に記録するデータに埋め込む請求の範囲第２７項記載の記録媒体の記録装置。

２９．上記制御部は、上記メモリから読み出された使用者識別データを暗号化して上記記録媒体に記録するデータに埋め込む請求の範囲第２８項記載の記録媒体の記録装置。

３０．上記メモリは、ユーザによって設定された使用者識別データが書きこまれる請求の範囲第１８項記載の記録媒体の記録装置。

３１．上記メモリに記憶される使用者識別データは、ユーザによって設定される請求の範囲第１８項記載の記録媒体の記録装置。

３２．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第３１項記載の記録媒体の記録装置。

３３．データとともに使用者を特定するための使用者識別データが記録された記録媒体から読み出された上記使用者識別データと上記記録媒体の再生時に装置から読み出された使用者識別データとを比較し、

上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記記録媒体の再生を行う記録媒体の再生方法。

３４．上記記録媒体には、更に上記記録媒体の再生動作を管理するための管理データが記録されており、上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記記録媒体から読み出された上記管理データに基づいて上記記録媒体の再生を行う請求の範囲第３３項記載の記録媒体の再生方法。

３５．上記方法は、上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記記録媒体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第３４項記載の記録媒体の再生方法。

３６．上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第３５項記載の記録媒体の再生方法。

３７．上記記録媒体には暗号化処理が施されたデータが記録されており、上記方法は上記記録媒体から読み出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときには、上記記録媒体から読み出されたデータに施されている暗号処理を上記使用者識別データを用いて復号処理を行う請求の範囲第３３項記載の記録媒体の再生方法。

３８．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第３３項記載の記録媒体の再生方法。

３９．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第３８項記載の記録媒体の再生方法。

４０．暗号化処理が施されたデータとともに少なくとも使用者を特定するための使用者識別データと再生管理データが記録された記録媒体を走査するヘッド部と、

使用者識別データが記憶されたメモリと、

上記ヘッド部によって上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとを比較し、上記比較結果に基づいて上記記録媒体の再生動作を制御する制御部とを備えている記録媒体の再生装置。

４１．上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときに、上記記録媒体の再生を行う請求の範囲第４０項記載の記録媒体の再生装置。

４２．上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致したときには、上記ヘッド部によって上記記録媒体から読み出されたデータに施されている暗号化処理を上記使用者識別データを用いて復号する請求の範囲第４１項記載の記録媒体の再生装置。

４３．上記制御部は、上記ヘッド部によって上記記録媒体から読み出された使用者識別データが検出できなかったときには、上記記録媒体から読み出された上記再生管理データに基づいて上記記録媒体の再生動作を制御する請求の範囲第４２項記載の記録媒体の再生装置。

４４．上記メモリは、上記装置に接続される使用者識別データ提供部に設けられている請求の範囲第４０項記載の記録媒体の再生装置。

４５．上記制御部は、上記装置に上記提供部が接続されていると判別されたときには上記提供部との間で認証処理を行う請求の範囲第４０項記載の記録媒体の再生装置。

４６．上記制御部は、上記認証処理が正しく終了したときには上記提供部に上記メモリから上記使用者識別データを読み出すように指示をする請求の範囲第４５項記載の記録媒体の再生装置。

４７．上記メモリから読み出された使用者識別データは暗号化処理が施されて、上記提供部から上記制御部に送信される請求の範囲第４６項記載の記録媒体の再生装置。

４８．上記制御部は、上記認証処理が正しく終了できなかったときには上記記録媒体の記録動作を中止する請求の範囲第４５項記載の記録媒体の再生装置。

４９．上記制御部は、上記装置に上記提供部が接続されていないと判別されたときには使用者に上記制御部を接続するように告知する請求の範囲第４０項記載の記録媒体の再生装置。

５０．上記制御部は、上記記録媒体から読み出された使用者識別データと上記メモリから読み出された使用者識別データとが一致しなかったときに、上記記録媒

体から読み出された使用者識別データが特定の識別データであったときには、上記記録媒体の再生を許可する請求の範囲第４１項記載の記録媒体の再生装置。

５１．上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第５０項記載の記録媒体の再生装置。

５２．上記メモリには、使用者によって設定された上記使用者識別データが書きこまれる請求の範囲第５０項記載の記録媒体の再生装置。

５３．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第４０項記載の記録媒体の再生装置。

５４．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第５３項記載の記録媒体の再生装置。

５５．使用者を特定するための使用者識別データが少なくとも埋めこまれたデータから読み出された上記使用者識別データと上記データの複製動作を行う際に装置から読み出された使用者識別データとを比較し、

上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記データの出力制御を行うデータの複製制御方法。

５６．上記データには、更に上記データの複製動作を管理するための管理データを含んでおり、上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときには、上記管理データに基づいて上記データの複製動作を制御する請求の範囲第５５項記載のデータの複製制御方法。

５７．上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記装置から読み出された使用者識別データを暗号鍵として上記識別データに暗号化処理を施して出力する請求の範囲第５６項記載のデータの複製制御方法。

５８．上記方法は、上記装置から読み出された使用者識別データを上記データに埋め込む請求の範囲第５７項記載のデータの複製制御方法。

５９．上記方法は、上記装置から読み出された使用者識別データを暗号化して上記データに埋め込む請求の範囲第５７項記載のデータの複製制御方法。

６０．上記方法は、上記管理データが上記データの複製を行うにあたって課金処理が必要であることを示しているときには、課金処理が可能であるか否かを判別し、上記判別結果が課金処理可能であることを示しているときに複製を実行する請求の範囲第５６項記載のデータの複製制御方法。

６１．上記方法は、上記課金処理は複製可能回数を示す度数を減算することによって行われる請求の範囲第６０項記載のデータの複製制御方法。

６２．上記方法は、上記課金処理が不可能であると判別であると判別されたときで、上記度数の加算が行われなかったときには複製動作を停止させる請求の範囲第６１項記載のデータの複製制御方法。

６３．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第５５項記載のデータの複製制御方法。

６４．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第６３項記載のデータの複製制御方法。

６５．少なくとも使用者を特定するための使用者識別データが埋めこまれたデータから抽出された上記使用者識別データと上記データの再生時に装置から読み出された使用者識別データを比較し、

上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときに、上記データの再生を行うデータの再生方法。

６６．上記データには、更に上記データの再生動作を管理するための管理データが記録されており、上記方法は、上記データから抽出された使用者識別データと上記装置から読み出され使用者識別データとが一致しなかったときには、上記管理データに基づいて上記データの再生を行う請求の範囲第６５項記載のデータの再生方法。

６７．上記方法は、上記データから使用者識別データが検出できなかったときには、上記再生管理データに基づいて上記データの再生動作を制御する請求の範囲第６６項記載のデータの再生方法。

６８．上記方法は、上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致しなかったときに、上記データから抽出された使用者識別データが特定の識別データであったときには、上記データの再

生を許可する請求の範囲の６６項記載のデータの再生方法。

６９．上記特定の識別データは、上記記録媒体がオリジナルの記録媒体であることを示す識別データである請求の範囲第６８項記載のデータの再生方法。

７０．上記方法は、上記管理データが上記データの再生を行うにあたって課金処理が必要であることを示しているときには、課金処理が可能であるか否かを判別し、上記判別結果が課金処理可能であることを示しているときに上記データの再生を実行する請求の範囲第６６項記載のデータの再生方法。

７１．上記方法は、上記課金処理は再生可能回数を示す度数を減算することによって行われる請求の範囲第７０記載のデータの再生方法。

７２．上記方法は、上記課金処理が不可能であると判別であると判別されたときで、上記度数の加算が行われなかったときには再生動作を禁止する請求の範囲第７１項記載のデータの再生方法。

７３．上記データには暗号化処理が施されたデータが記録されており、上記方法は上記データから抽出された使用者識別データと上記装置から読み出された使用者識別データとが一致したときには、上記抽出されたデータに施されている暗号処理を上記使用者識別データを用いて復号処理を行う請求の範囲第６５項記載のデータの再生方法。

７４．上記装置から読み出される使用者識別データは、ユーザによって設定される請求の範囲第６５項記載のデータの再生方法。

７５．上記使用者識別データは、ユーザ名を含むデータである請求の範囲第７４項記載のデータ再生方法。

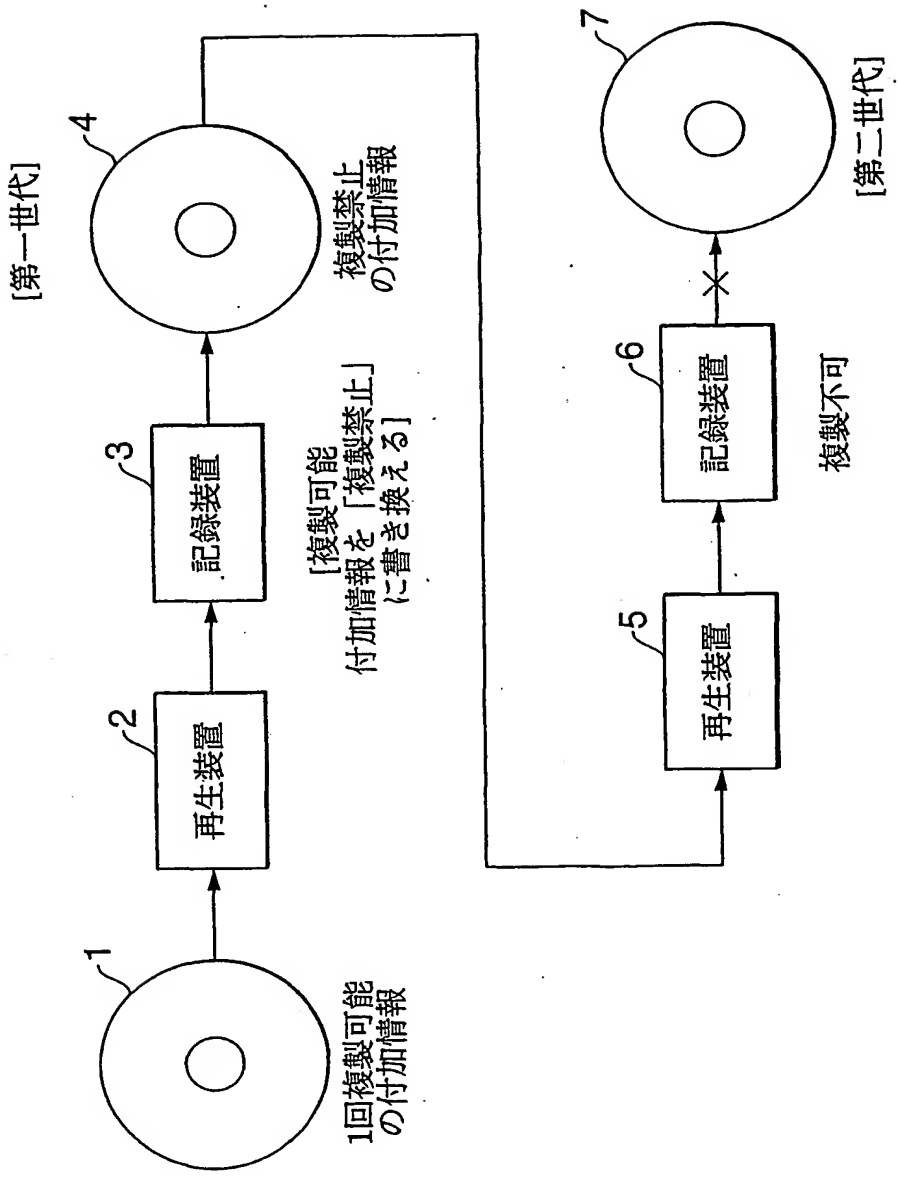

[第一世代]
1
1回複製可能
の付加情報
2
再生装置
3
記録装置
[複製可能
付加情報を「複製禁止」
に書き換える]
4
複製禁止
の付加情報
5
再生装置
6
記録装置
複製不可
7
[第二世代]

FIG.1

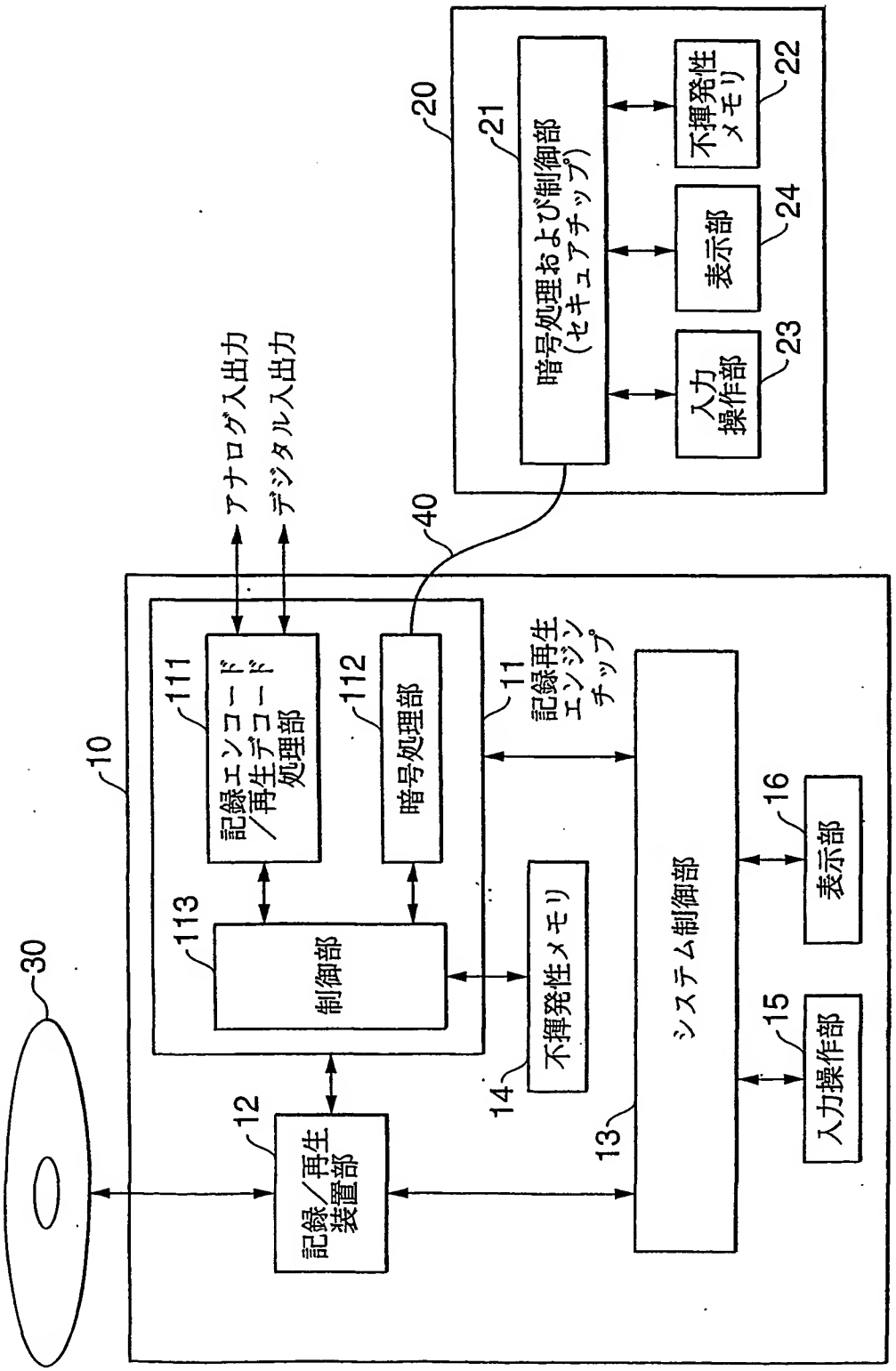

30
10
アナログ入出力
デジタル入出力
111
記録エンコード
再生デコード
処理部
112
暗号処理部
113
制御部
11
記録再生
エンジン
チップ
12
記録／再生
装置部
14
不揮発性メモリ
13
システム制御部
16
表示部
15
入力操作部
40
20
21
暗号処理および制御部
(セキュアチップ)
22
不揮発性
メモリ
24
表示部
23
入力
操作部

FIG.2

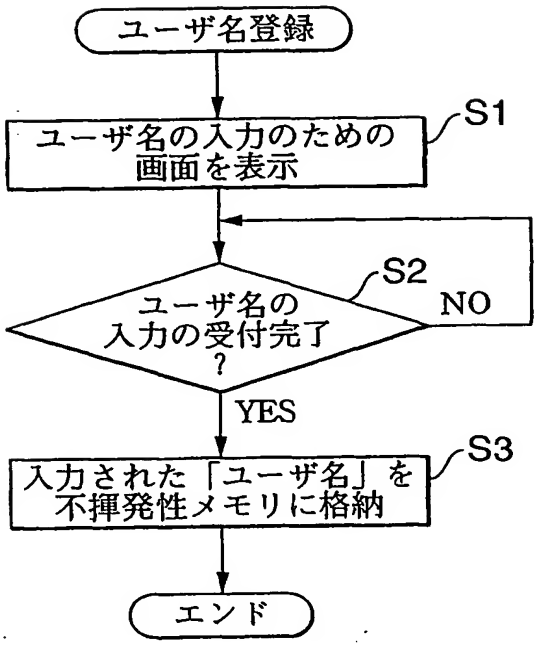

ユーザ名登録
ユーザ名の入力のための画面を表示
S1
ユーザ名の入力の受付完了？
S2
NO
YES
入力された「ユーザ名」を不揮発性メモリに格納
S3
エンド

FIG.3

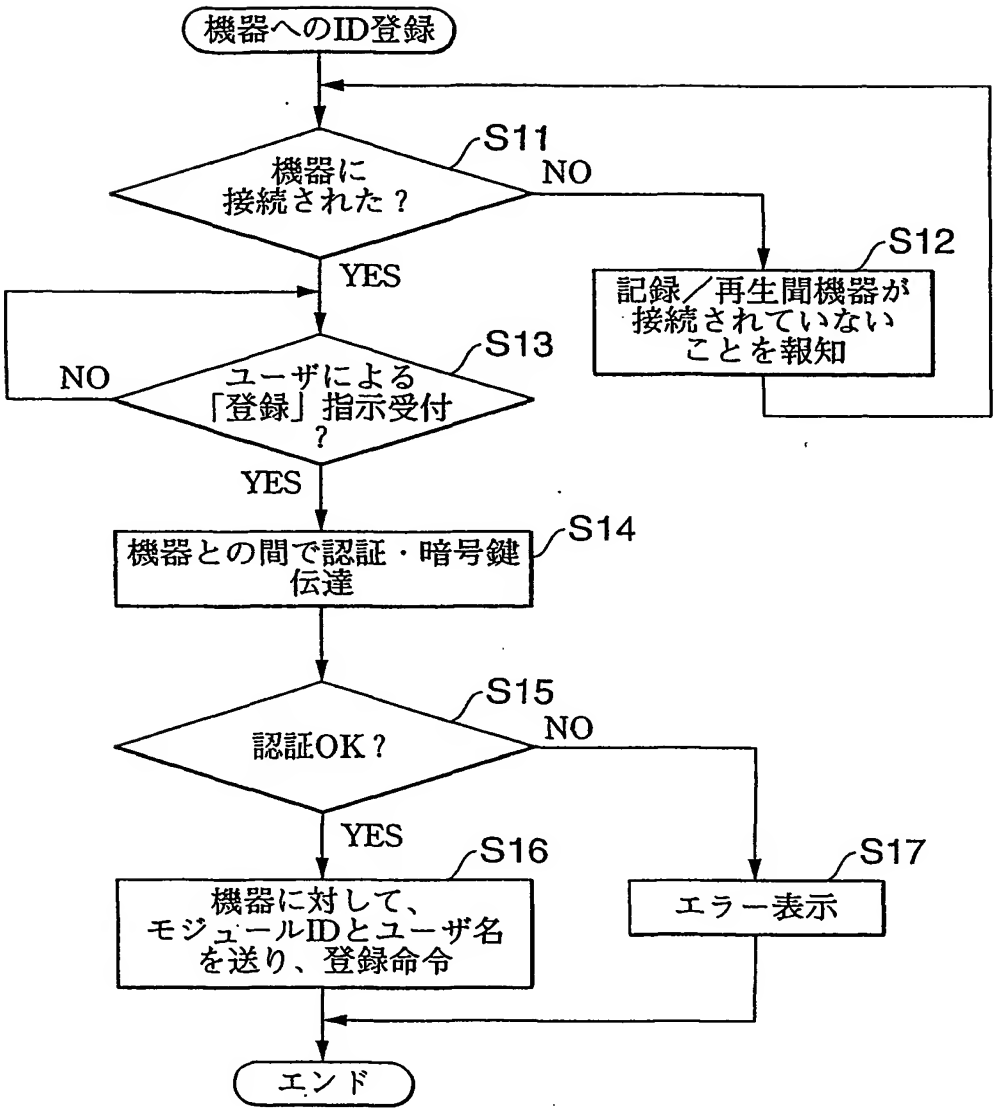

機器へのID登録
S11
機器に
接続された？
NO
S12
記録／再生聞機器が
接続されていない
ことを報知
YES
S13
NO
ユーザによる
「登録」指示受付
？
YES
S14
機器との間で認証・暗号鍵
伝達
S15
認証OK？
NO
YES
S16
機器に対して、
モジュールIDとユーザ名
を送り、登録命令
S17
エラー表示
エンド

FIG.4

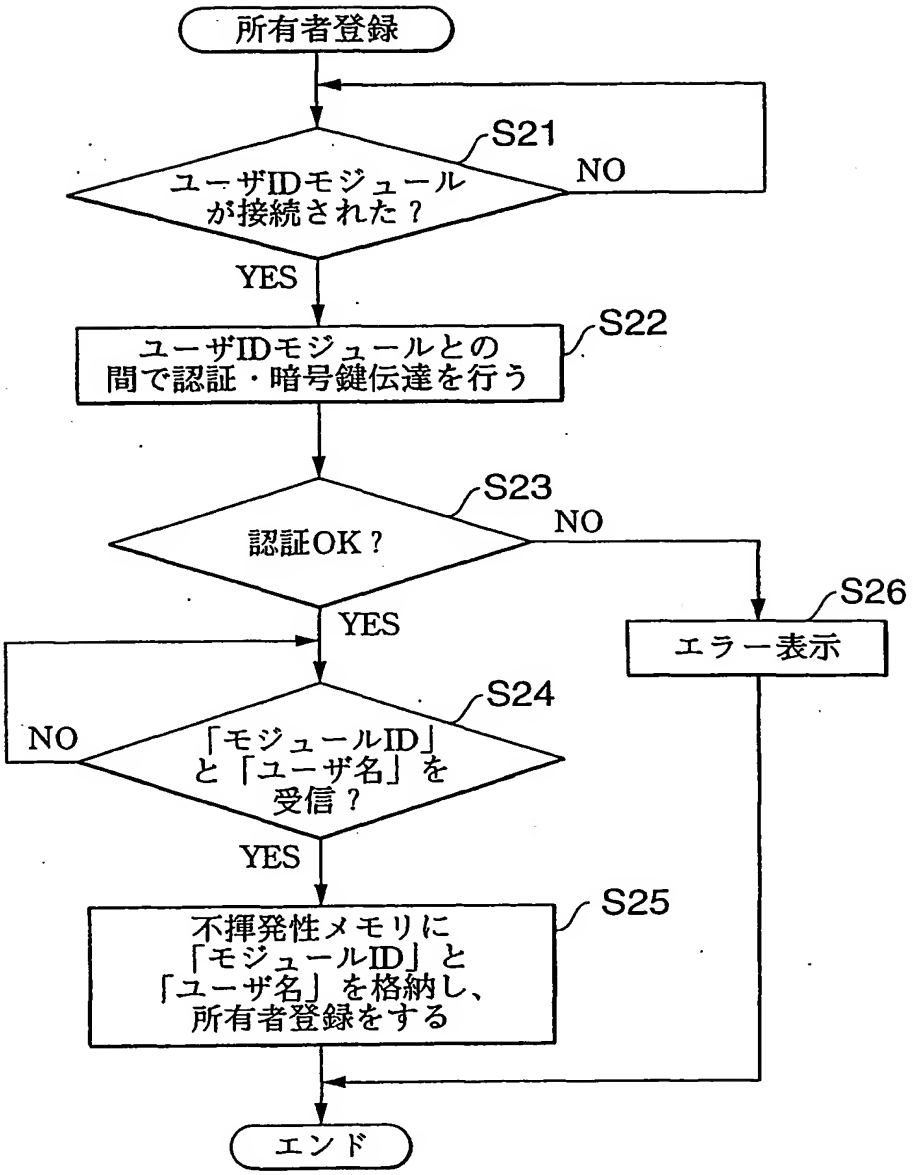

所有者登録
S21
ユーザIDモジュール
が接続された？
NO
YES
S22
ユーザIDモジュールとの
間で認証・暗号鍵伝達を行う
S23
認証OK？
NO
YES
S26
エラー表示
S24
「モジュールID」
と「ユーザ名」を
受信？
NO
YES
S25
不揮発性メモリに
「モジュールID」と
「ユーザ名」を格納し、
所有者登録をする
エンド

FIG.5

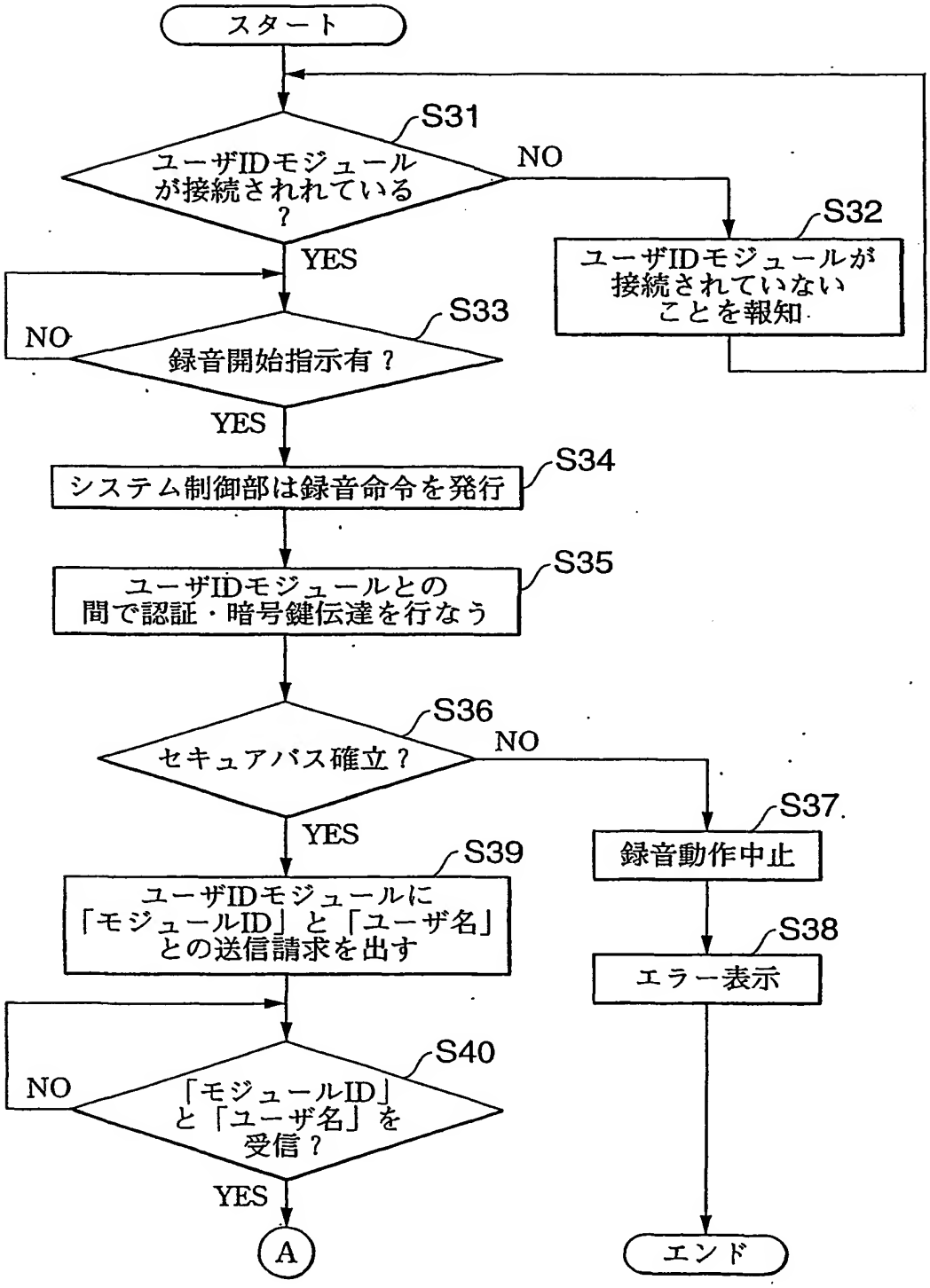

スタート
S31
ユーザIDモジュール
が接続されれている
?
NO
S32
ユーザIDモジュールが
接続されていない
ことを報知
YES
S33
NO
録音開始指示有？
YES
S34
システム制御部は録音命令を発行
S35
ユーザIDモジュールとの
間で認証・暗号鍵伝達を行なう
S36
セキュアパス確立？
NO
S37
録音動作中止
YES
S39
ユーザIDモジュールに
「モジュールID」と「ユーザ名」
との送信請求を出す
S38
エラー表示
S40
NO
「モジュールID」
と「ユーザ名」を
受信？
YES
A
エンド

FIG.6

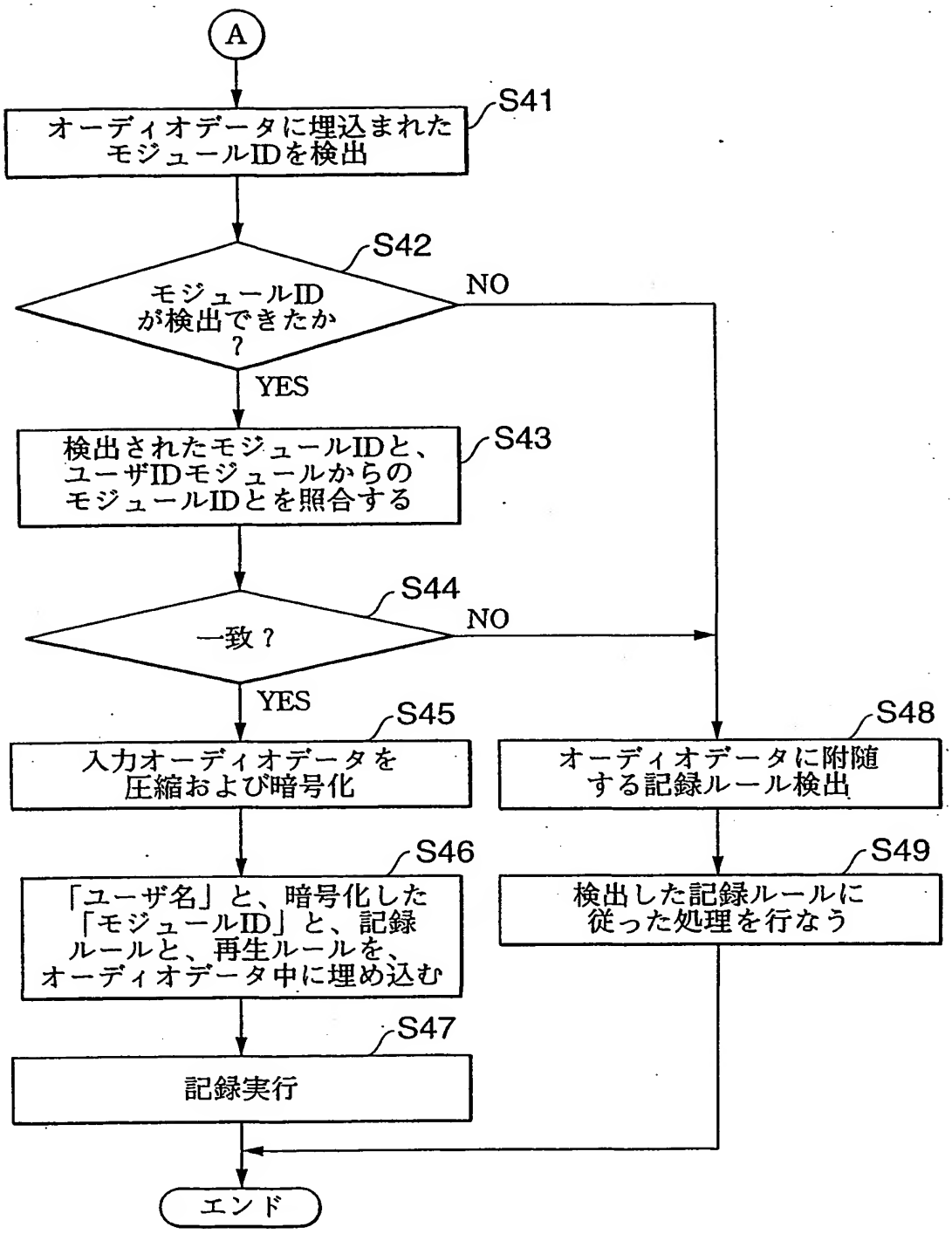

A
S41
オーディオデータに埋込まれた
モジュールIDを検出
S42
モジュールID
が検出できたか
?
NO
YES
S43
検出されたモジュールIDと、
ユーザIDモジュールからの
モジュールIDとを照合する
S44
一致?
NO
YES
S45
入力オーディオデータを
圧縮および暗号化
S46
「ユーザ名」と、暗号化した
「モジュールID」と、記録
ルールと、再生ルールを、
オーディオデータ中に埋め込む
S47
記録実行
S48
オーディオデータに附随
する記録ルール検出
S49
検出した記録ルールに
従った処理を行なう
エンド

FIG.7

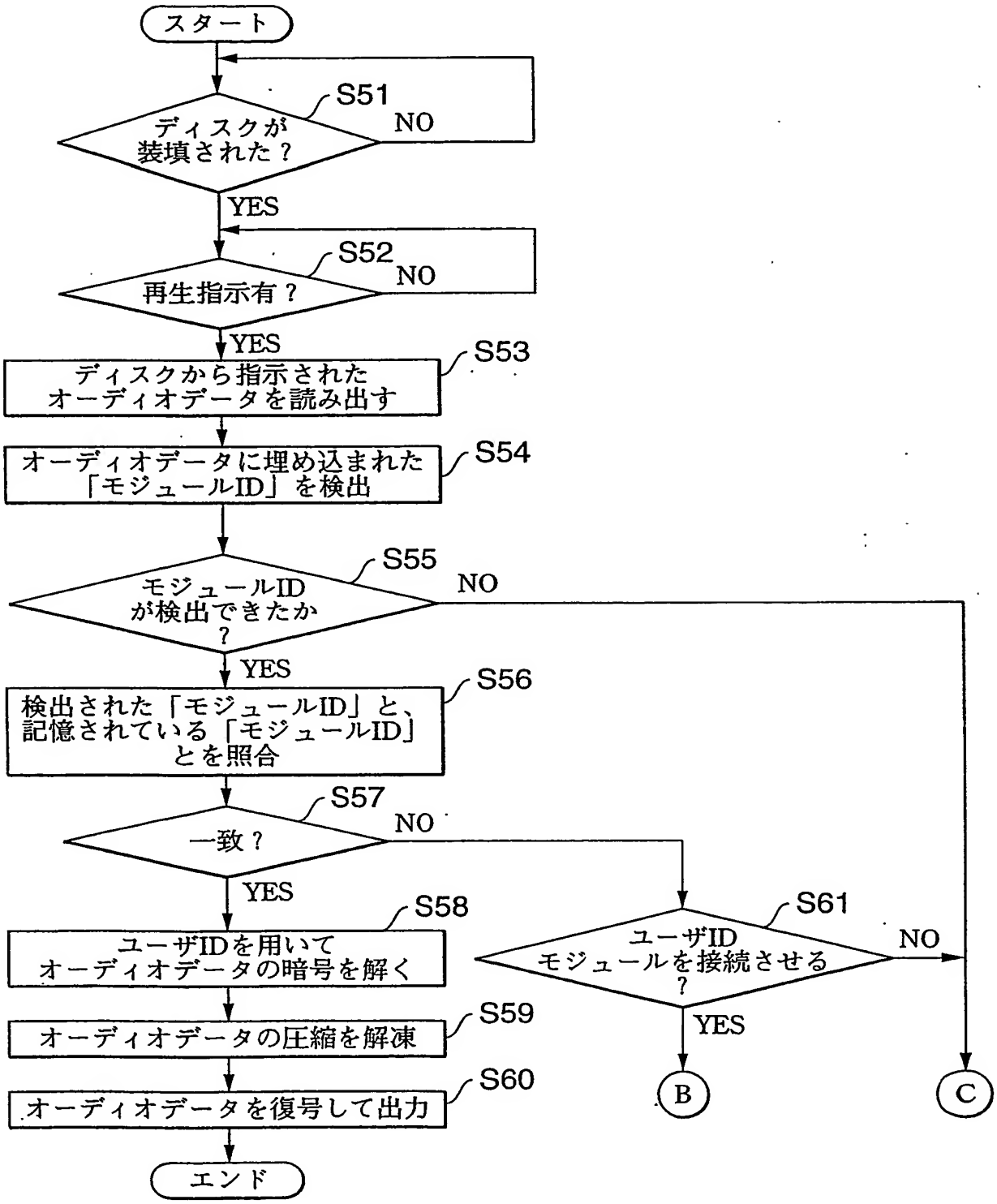

スタート
S51
ディスクが装填された？
NO
YES
S52
再生指示有？
NO
YES
S53
ディスクから指示されたオーディオデータを読み出す
S54
オーディオデータに埋め込まれた「モジュールID」を検出
S55
モジュールIDが検出できたか？
NO
YES
S56
検出された「モジュールID」と、記憶されている「モジュールID」とを照合
S57
一致？
NO
YES
S58
ユーザIDを用いてオーディオデータの暗号を解く
S59
オーディオデータの圧縮を解凍
S60
オーディオデータを復号して出力
エンド
S61
ユーザIDモジュールを接続させる？
NO
YES
B
C

FIG.8

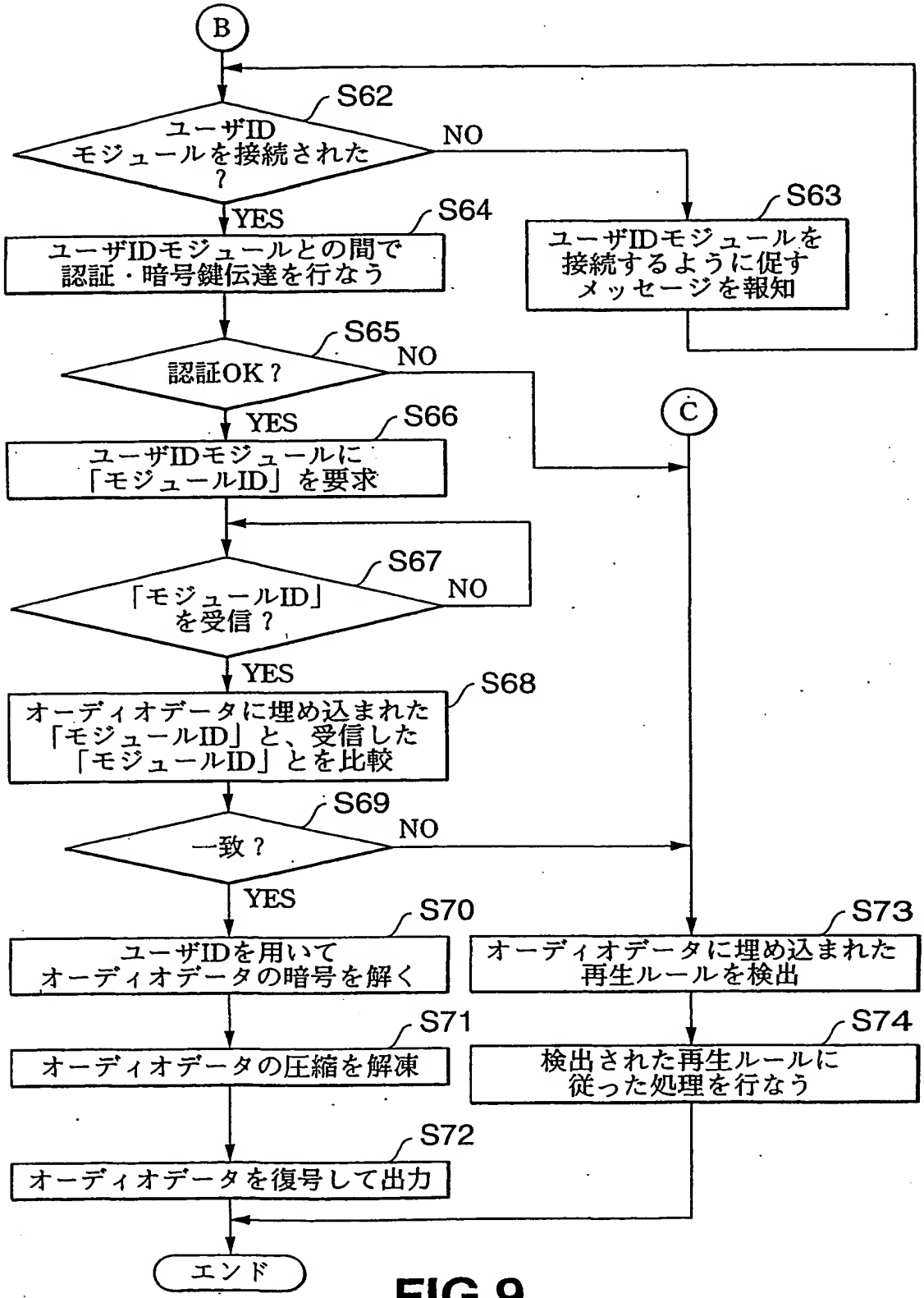

B
S62
ユーザID
モジュールを接続された
?
NO
YES
S64
ユーザIDモジュールとの間で
認証・暗号鍵伝達を行なう
S63
ユーザIDモジュールを
接続するように促す
メッセージを報知
S65
認証OK?
NO
YES
S66
ユーザIDモジュールに
「モジュールID」を要求
C
S67
「モジュールID」
を受信?
NO
YES
S68
オーディオデータに埋め込まれた
「モジュールID」と、受信した
「モジュールID」とを比較
S69
一致?
NO
YES
S70
ユーザIDを用いて
オーディオデータの暗号を解く
S73
オーディオデータに埋め込まれた
再生ルールを検出
S71
オーディオデータの圧縮を解凍
S74
検出された再生ルールに
従った処理を行なう
S72
オーディオデータを復号して出力
エンド

FIG.9

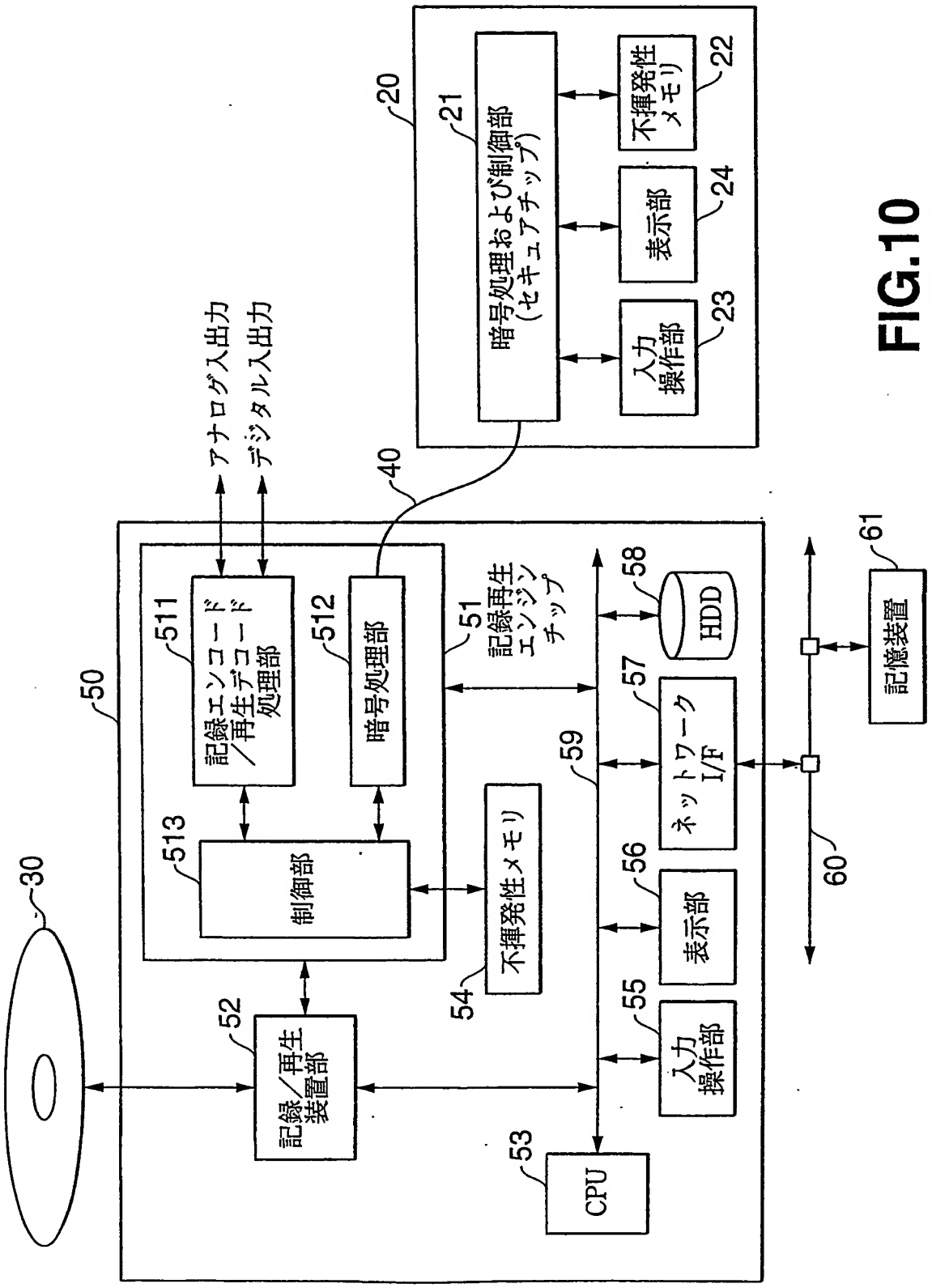

20
21
暗号処理および制御部
(セキュアチップ)
不揮発性メモリ
22
表示部
24
入力操作部
23
アナログ入出力
デジタル入出力
40
50
511
記録エンコード/再生デコード処理部
512
暗号処理部
51
記録再生エンジンチップ
58
HDD
57
ネットワークI/F
61
記憶装置
59
513
制御部
不揮発性メモリ
54
56
表示部
60
30
52
記録/再生装置部
55
入力操作部
53
CPU

FIG.10

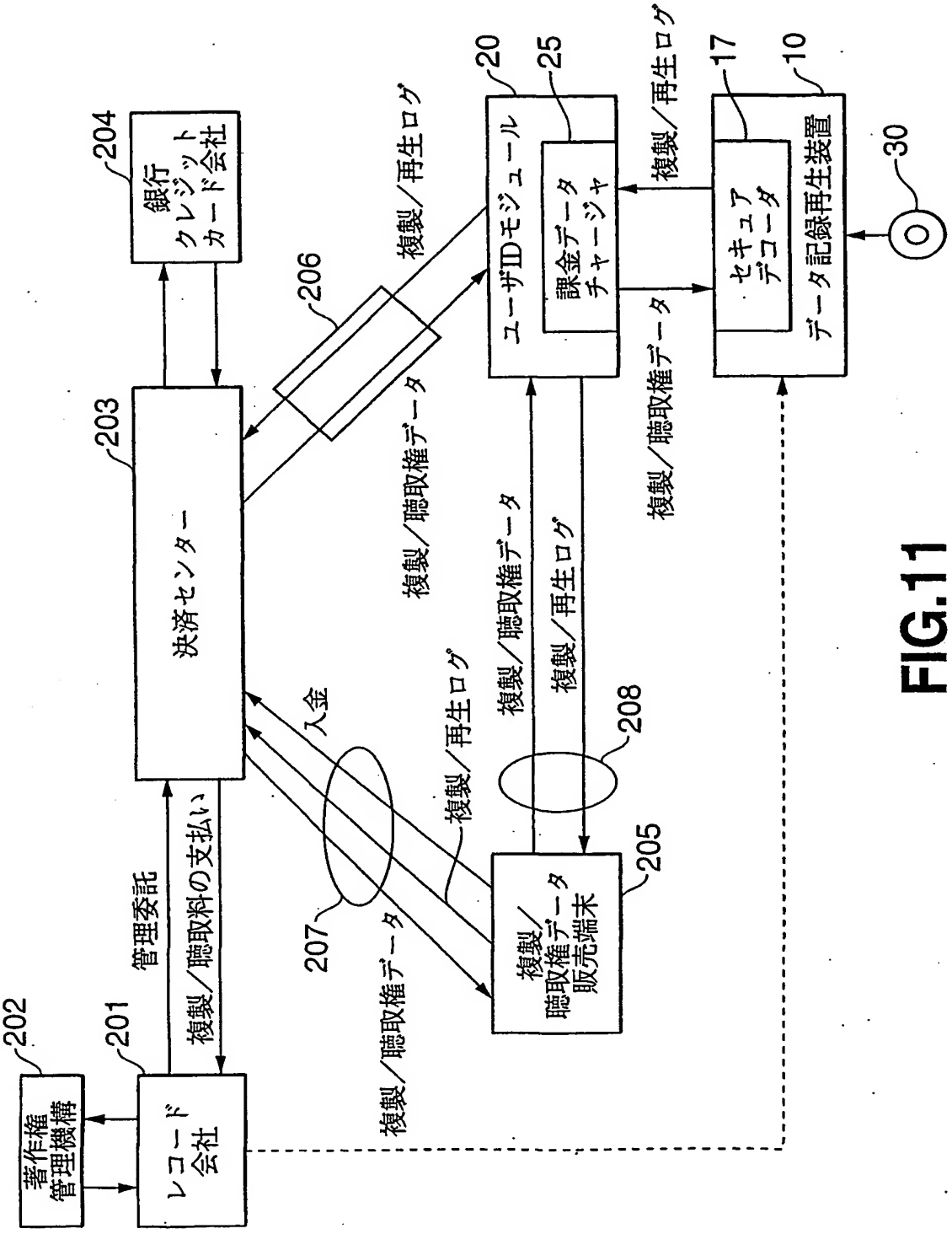

著作権管理機構
202
レコード会社
201
管理委託
複製／聴取料の支払い
決済センター
203
銀行クレジットカード会社
204
入金
207
複製／聴取権データ
複製／再生ログ
206
複製／聴取権データ
複製／再生ログ
複製／聴取権データ
複製／再生ログ
208
複製／聴取権データ販売端末
205
ユーザIDモジュール
20
課金データチャージャ
25
セキュアデコーダ
17
データ記録再生装置
10
30
複製／聴取権データ
複製／再生ログ

FIG.11

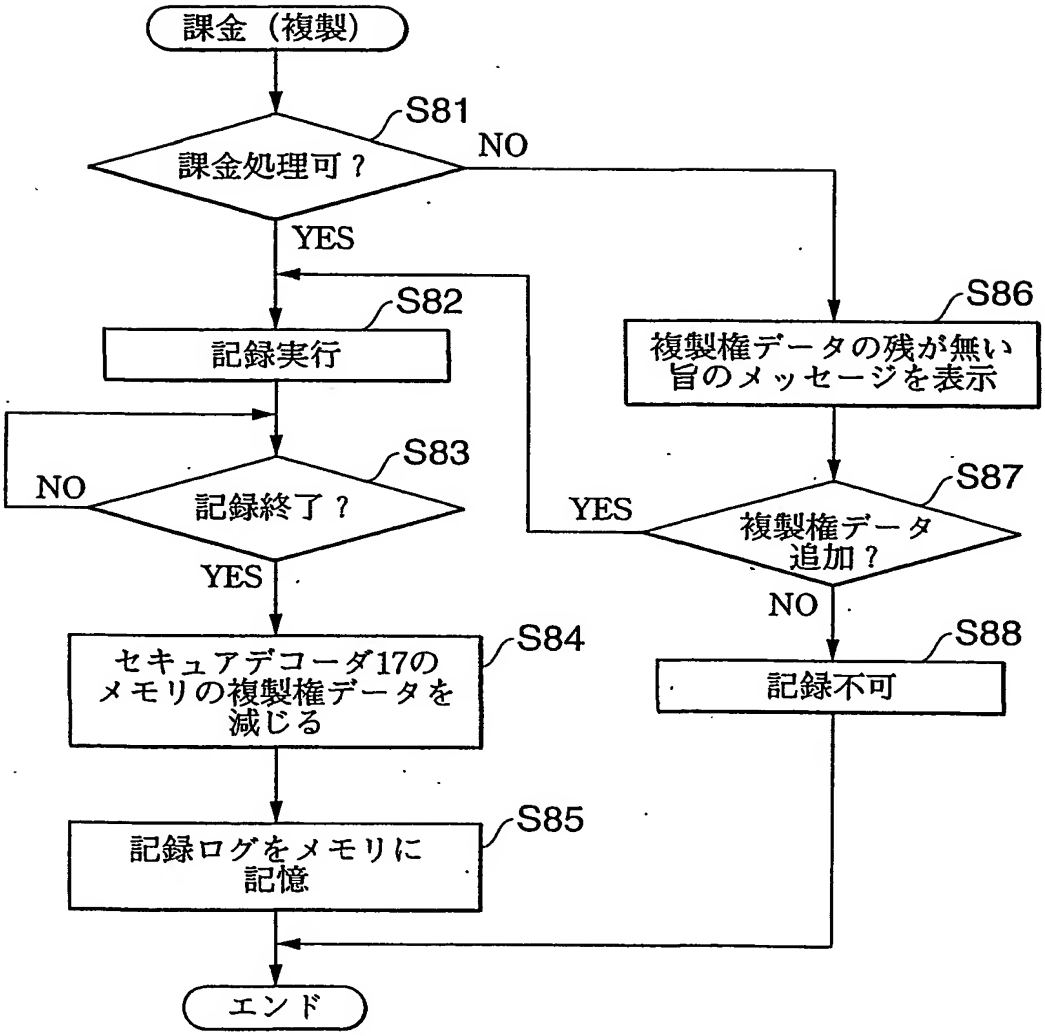

課金（複製）
S81
課金処理可？
NO
YES
S82
記録実行
S83
NO
記録終了？
YES
S84
セキュアデコーダ17の
メモリの複製権データを
減じる
S85
記録ログをメモリに
記憶
エンド
S86
複製権データの残が無い
旨のメッセージを表示
S87
YES
複製権データ
追加？
NO
S88
記録不可

FIG.12

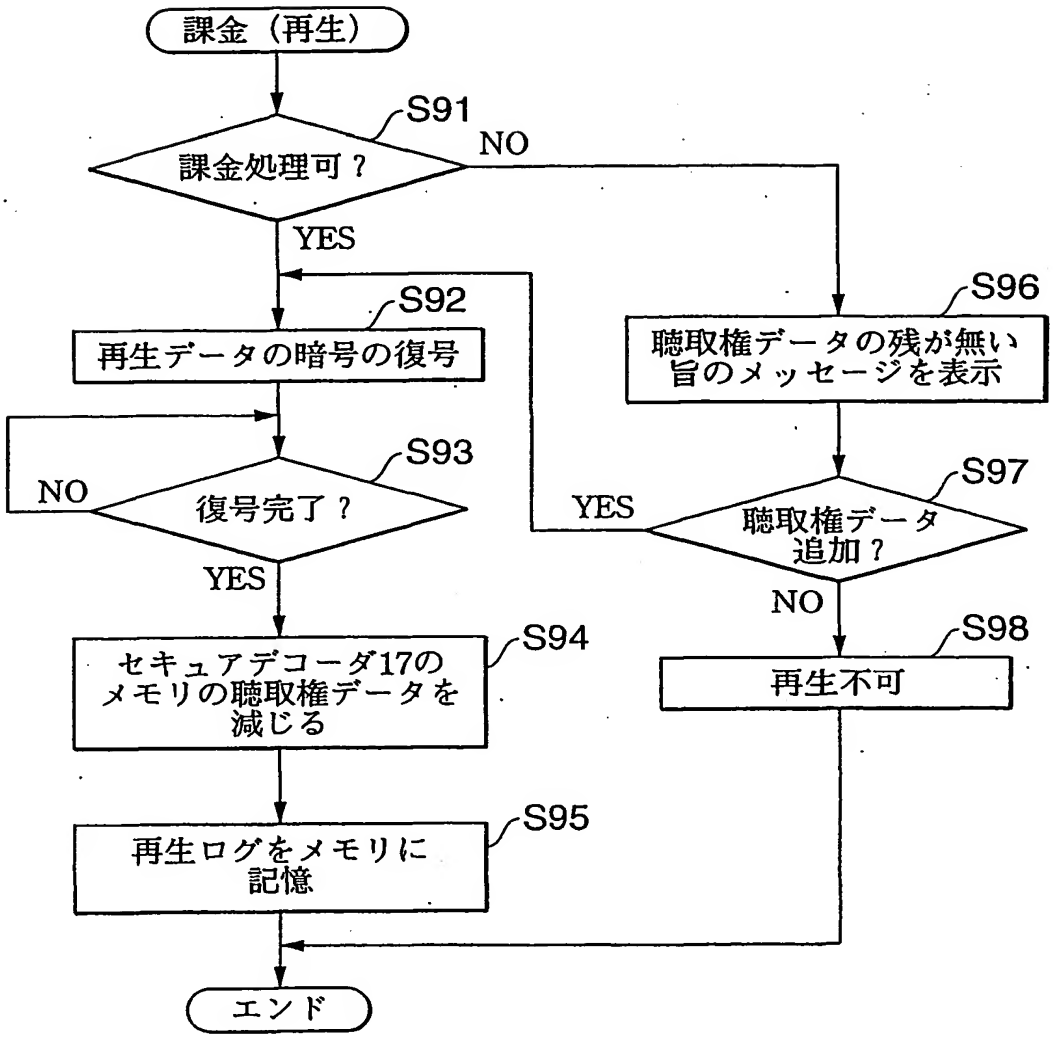

課金（再生）
S91
課金処理可？
NO
YES
S92
再生データの暗号の復号
S93
NO
復号完了？
YES
S94
セキュアデコーダ17の
メモリの聴取権データを
減じる
S95
再生ログをメモリに
記憶
エンド
S96
聴取権データの残が無い
旨のメッセージを表示
S97
聴取権データ
追加？
YES
NO
S98
再生不可

FIG.13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/06183

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G11B 20/10, G10F 3/06, G06F 17/60, G10K 15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G11B 20/10, H04N 5/91, G10F 3/06, G06F 17/60, G10K 15/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-238306 A (Fujitsu Limited), 31 August, 1999 (31.08.99), Full text; Figs. 1 to 18 & EP 000930616 A2 & CN 001227948 A	1-75
Y	JP 10-208388 A (Victor Company of Japan, Limited), 07 August, 1998 (07.08.98), Full text; Figs. 1 to 7 & EP 000853315 A2 & US 006097814 A1	1-75
Y	JP 11-306672 A (Sony Corporation), 05 November, 1999 (05.11.99), Full text; Figs. 1 to 8 (Family: none)	1-75
Y	JP 2000-113587 A (Sony Corporation), 21 April, 2000 (21.04.00), Full text; Figs. 1 to 10 (Family: none)	1-75
A	JP 2000-195161 A (Victor Company of Japan, Limited), 14 July, 2000 (14.07.00), Full text; Figs. 1 to 11 (Family: none)	1-75

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 October, 2001 (03.10.01)	16 October, 2001 (16.10.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/06183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-213554 A (Toshiba Corporation), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 22 & CN 001220460 A	7-8,35-36, 50-51,68-69
A	JP 2000-156036 A (Sony Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 1 to 5 (Family: none)	20-25,44-49
A	JP 11-313282 A (Sanyo Electric Co., Ltd.), 09 November, 1999 (09.11.99), Full text; Figs. 1 to 16 & EP 000954173 A1	60-62,70-72

国際調査報告

国際出願番号 PCT／JP01／06183

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G11B 20／10 G10F 3／06 G06F 17／60
G10K 15／02

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G11B 20／10 H04N 5／91 G10F 3／06
G06F 17／60 G10K 15／02

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2001年
日本国登録実用新案公報 1994－2001年
日本国実用新案登録公報 1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 11-238306 A（富士通株式会社） 31. 8月. 1999 (31. 08. 99) 全文 第1－18図 & EP 000930616 A2 & CN 001227948 A	1-75
Y	JP 10-208388 A（日本ビクター株式会社） 7. 8月. 1998 (07. 08. 98) 全文 第1－7図 & EP 000853315 A2 & US 006097814 A1	1-75

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
03.10.01	16.10.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	宮下 誠 印	5Q	2946
	電話番号 03－3581－1101. 内線 3589		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP01／06183

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	ＪＰ　11-306672　Ａ（ソニー株式会社） 5．11月．1999（05．11．99） 全文　第1－8図　（ファミリーなし）	1-75
Y	ＪＰ　2000-113587　Ａ（ソニー株式会社） 21．4月．2000（21．04．00） 全文　第1－10図　（ファミリーなし）	1-75
A	ＪＰ　2000-195161　Ａ（日本ビクター株式会社） 14．7月．2000（14．07．00） 全文　第1－11図　（ファミリーなし）	1-75
A	ＪＰ　11-213554　Ａ（株式会社東芝） 6．8月．1999（06．08．99） 全文　第1－22図 ＆　ＣＮ　001220460　Ａ	7-8、35-36、50-51、68-69
A	ＪＰ　2000-156036　Ａ（ソニー株式会社） 6．6月．2000（06．06．00） 全文　第1－5図　（ファミリーなし）	20-25、44-49
A	ＪＰ　11-313282　Ａ（三洋電機株式会社） 9．11月．1999（09．11．99） 全文　第1－16図 ＆　Ｅ.Ｐ　000954173　Ａ１	60-62、70-72